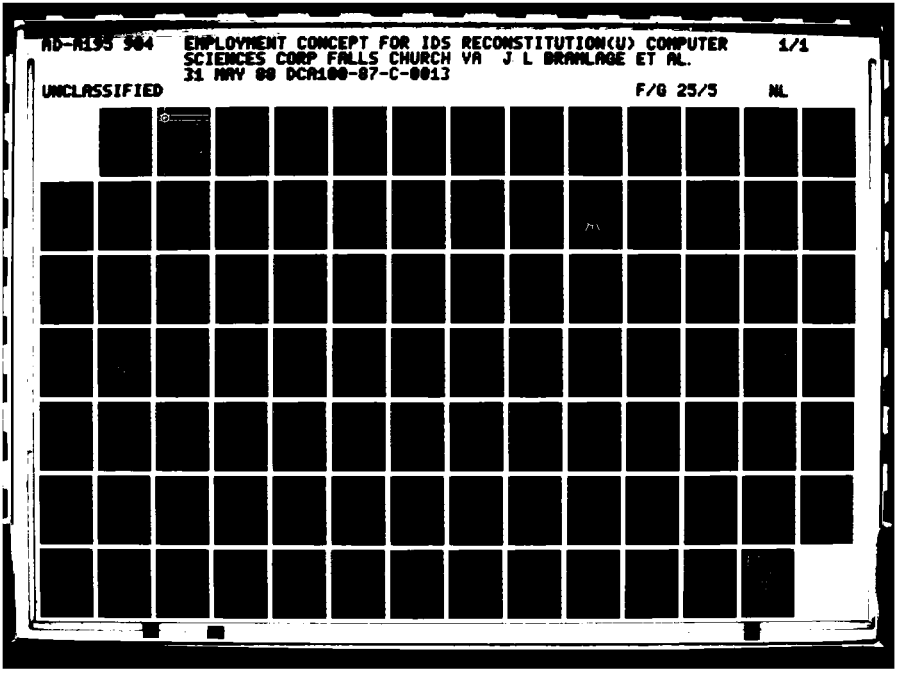
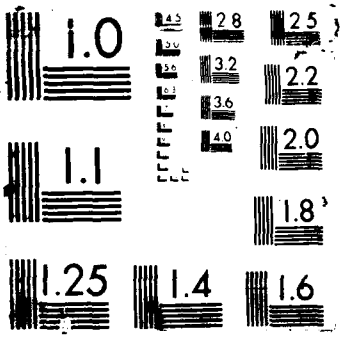

AD-A193 504
EMPLOYMENT CONCEPT FOR IDS RECONSTITUTION(U) COMPUTER SCIENCES CORP FALLS CHURCH VA J L BRANLAGE ET AL.
31 MAY 88 DCA100-87-C-0013
1/1
UNCLASSIFIED
F/G 25/5
NL


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0

(2)

DEFENSE COMMUNICATIONS ENGINEERING CENTER

EMPLOYMENT CONCEPT FOR IDS RECONSTITUTION

MAY 1988

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS None
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT Unlimited
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION Computer Sciences Corporation 6b. OFFICE SYMBOL (If applicable) 613	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State and ZIP Code) 3160 Fairview Park Drive Falls Church, VA 22042	7b. ADDRESS (City, State and ZIP Code)
8a. NAME OF FUNDING/SPONSORING ORGANIZATION Defense Communications Agency 8b. OFFICE SYMBOL (If applicable) R640	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER DCA100-87-C-0013
8c. ADDRESS (City, State and ZIP Code) 8th & South Courthouse Road Arlington, VA 22204	10. SOURCE OF FUNDING NOS. PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT NO.
11. TITLE (Include Security Classification) Employment Concept for IDS Reconstitution (U)	
12. PERSONAL AUTHOR(S) Bramlage, Judith L.; Roix, Robert; Brown, David; Arnaud, Daniel; Park, Jack; Wilmot, Roger	
13a. TYPE OF REPORT Final Technical 13b. TIME COVERED FROM JAN 87 TO MAY 88	14. DATE OF REPORT (Yr., Mo., Day) 1988 May 31 15. PAGE COUNT 150
16. SUPPLEMENTARY NOTATION	
17. COSATI CODES FIELD / GROUP / SUB GR.	18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number) DDN, Reconstitution, IDS

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

The DCS data service network supports DoD data communications services. When day-to-day measures are interrupted, critical C^2 users will require the network to be reconstituted to an acceptable level of service. The purpose of reconstitution planning is to ensure that sufficient resources are available to restore data user services to surviving critical DoD C^2 subscribers.

This document outlines the current network, defines reconstitution requirements, and offers recommendations to meet said requirements. These recommendations can be thought of as a planning framework that must be further explored and documented in order to develop a complete planning strategy for DDN reconstitution in a stressed environment.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT ☐ DTIC USERS ☐	21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a NAME OF RESPONSIBLE INDIVIDUAL Patrick Sullivan	22b TELEPHONE NUMBER (Include Area Code) (703) 437-2578 22c. OFFICE SYMBOL R640

DD FORM 1473, 83 APR EDITION OF 1 JAN 73 IS OBSOLETE.

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

EMPLOYMENT CONCEPT FOR IDS RECONSTITUTION

TECHNICAL REPORT
FINAL

TASK ORDER 86-11B

Prepared for:

DEFENSE COMMUNICATIONS AGENCY
DEFENSE COMMUNICATIONS ENGINEERING CENTER
1860 WIEHLE AVENUE
RESTON, VIRGINIA 22090

Prepared by:

COMPUTER SCIENCES CORPORATION
DEFENSE COMMUNICATIONS SYSTEMS OPERATION
6565 ARLINGTON BOULEVARD
FALLS CHURCH, VIRGINIA 22046

31 May 1988

CONTRACT NO.: DCA100-87-C-0013

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Continued)

LIST OF TABLES

LIST OF FIGURES

EXECUTIVE SUMMARY

The primary provider of data communications services to the DoD community is the Defense Communications System (DCS) data service network, which is charged with supporting DoD data users. Normal operations include redundancy, alternate routing, and highly distributed robust networks -- highly flexible and reliable measures taken to support day-to-day operational users. However, when these measures are no longer sufficient and data services are disrupted during times of stress, critical command and control (C^2) users will require the network to be reconstituted to an acceptable level of service, commensurate with the surviving forces. The purpose of reconstitution planning is to ensure that sufficient resources are available to restore data user services to surviving critical DoD C^2 subscribers. Planning for reconstitution must start at the physical level and begin with a basic understanding of the interrelated elements of the DCS. Reconstitution of the DCS data system must be accomplished in harmony with the existing reconstitution plans of all other elements of the DCS. This document surveys existing, planned, and potentially emerging interconnect technologies, services, and components that could be employed to provide the requisite interconnect facilities to support reconstitution of the DCS data system. In doing so, it illustrates the intricacies of reconstitution planning; these interconnect facilities are used for all DCS users and are not solely dedicated to the data community. During times of stress, all surviving interconnect resources are subject to strict allocation procedures controlled by the Executive Office of the President through the National Communications System (NCS).

Because crisis scenarios are so varied, and because it is impossible to predict which facilities will survive what crisis levels, the reconstitution strategies identified herein are not aimed at the complete range of original services, but are focused on high priority critical networks and the C^2 users. The quality of communications can be expected to be reduced -- this includes lower data rates and longer delays.

This report focuses on five available, emerging technologies and examines them in relation to their applicability to IDS reconstitution and, specifically, to reconnection of users to the network. The communications technologies included are: packet radio, very small aperture terminal (VSAT), high frequency radio, meteor burst, and switched telephone.

It is especially important that reconstitution plans and pre-crisis priorities be established. Since it is not possible to select the exact situation from the wide range of possible scenarios, and the specific circumstances cannot be predetermined, selection of a particular

interconnect media is not possible; this is not an either/or situation. The analysis presented herein provides the data network and engineering planning community with an understanding and appreciation of the magnitude of the planning requirements which surround the reconstitution process.

The future data network component of the DCS has three primary identifiable elements: terminals/data switches, interconnecting circuits, and operating plans/procedures. Reconstitution plans should be based on a balanced emphasis on all three. Further, these plans must build on existing DCS/NCS plans and procedures. Terminal/switch nodes must be flexible and be capable of interfacing with a variety of media. For example, existing and planned key nodal points should be equipped with a requisite suite of interface hardware to allow a given terminal/data switch to be interoperable with a variety of the types of interconnect media available at that specific geographical location.

During the planning process, critical users and switches -- coupled with information on available interconnect media -- must be identified. Some locations will be determined to have robust connectivity available, while others may require augmentation (through selective acquisition of limited dedicated data network reconstitution interconnect assets). A flexible and adaptable interconnect environment is imperative. At this time, it is not possible to determine what must be procured and where it must be deployed without an extensive indepth study of each site and the network user population.

In order for the DCS data network system to take maximum advantage of the various interconnect media that might be available, particular attention must be made to two important areas: (1) the acquisition of the physical interface between the terminal/switch components and the available media and (2) the National Security Emergency Preparedness (NSEP) Telecommunications Service Priority System (TSPS) rules for establishing appropriate restoration priority levels for an identified set of user categories.

After critical switch nodes are identified and prioritized, a review of the planning and potential development efforts for the acquisition and employment application of a replacement switch capability must be examined.

In addition to the reconstitution plans that surround the question of "What" should be done to prepare for reconstitution, another dimension of planning effort must also be addressed -- that of "How" to operate the data network during times of stress. This planning dimension can be categorized as the instructions and guidance necessary to operate in the expected environment. In a network that has few -- if any -- operating personnel (most of the switches will be unmanned), the procedures for reconnecting the surviving customers to a surviving switch and into the available interconnecting media will not be an easy task. "Who" is going to orchestrate the network/local area restoration activities and "Who" is going to accomplish the actions required to recreate the data services network? Many of the supporting communications facilities are converting to streamlined, digital, less man-

power-intensive equipment. Operating communications personnel who do remain on-site will be fully employed reconstituting and maintaining critical high level C^2 traffic. The requirements of the general services data network must be placed in perspective with all other telecommunications services and handled accordingly. The process of reestablishing the requisite databases and identifying addresses and subscribers must be made as simple as possible.

In summary, the recommendations contained in Section 6 emphasize and focus on additional areas that must be addressed in order to develop a complete *Reconstitution Planning Strategy* for the data services component of the DCS. These recommendations can be thought of as a first level planning framework that must be further explored and documented in order to develop a complete planning strategy for DDN reconstitution in a stressed environment. All of these recommendations must be fully examined prior to making any determinations about what to buy and where to use it. Development of any *Reconstitution Employment Strategies* must be accomplished after a plausible higher level planning framework has been developed that addresses the complex issues surrounding reconstitution and restoration of service to key C^2 customers.

This Page Left Blank Intentionally.

SECTION 1 - Introduction

1.1 Background

The concept of reconstitution is rooted in the National Security Decision Directive (NSDD) -97 and NSDD-47 documents[1], which establish general objectives and principles for reconstituting communications capabilities in crisis and stressed situations. The Defense Communications System (DCS), consisting of switched systems and transmission plant, is the primary provider of communications services to the DoD community. Switched systems include message switched (AUTODIN), packet switched (DDN) and circuit switched (DSN/AUTOVON). The DCS is being modernized and upgraded to meet new demands on a worldwide basis. A primary mission is to support the DoD command and control users in peace time and in times of stress. Consequently, it is postured to provide a high degree of availability, commensurate with user priorities, during various levels of stress. This is provided through redundancy, alternate routing and highly distributed robust networks. However, there are scenarios under which this system will fail and service to key subscribers would be interrupted. These situations are covered by reconstitution plans to ensure that resources are available to restore the service required by the surviving critical subscribers. This document addresses reconstitution of services provided by one major subsystem of the DCS, the DCS data system. This system, when fully integrated, will include the packet switched services of the various DDN subnets (e.g., MILNET and DISNET); the formal message service of the AUTODIN; gateway services; and other value-added data communications services and enhancements. The reconstitution of DCS data system will require the provision of data communications services to critical command, control and intelligence (C^2I) users during the stress levels identified in Paragraphs 3.4.2 and 3.4.3 of the DDN Program Plan.

The primary elements of the DCS data system are: the terminals/switches, the plans/procedures, network management/control, and the interconnects. Each key element of the DCS data system must receive equal consideration in reconstitution planning if it to succeed. In addition, user Continuity of Operations Plans (COOP) and reconstitution plans of other components of the DCS, as well as, the plans of national and international large scale communications systems must be considered in order to determine specific user requirements and to more effectively utilize the limited reconstitution assesses. However, the coordination and/or integration of these plans is outside the scope of this document.

---

1. NSDD-47, Emergency Mobilization Preparedness
   NSDD-97, National Security Telecommunications Policy

1.2 Purpose

The purpose of this document is to survey existing, planned, and potentially emerging interconnect technologies, services, and components that could be employed to provide the requisite interconnect facilities to support reconstitution of the DCS data system. This analysis for developing DCS data system reconstitution strategies includes a description of the communication systems environment (pre- and post-attack) and a survey of promising and near-term (1990 time frame) technologies, techniques, and assets which may be available either off the shelf or from other ongoing defense programs. Once these are identified, this document presents a generic application of these interconnect technologies for reconstitution of DCS data system services when faced with: (1) loss of special hosts, (2) loss of packet switch nodes, and/or (3) loss of supporting transmission connectivity. It must be remembered that the requirements for reconstitution of the DCS data system services are driven by the assumed survival of the end user and their COOP.

The reconstitution of the complete range of services to the surviving users that existed prior to the initiation of the conflict is not considered practical or doable in the post-attack or war environment. Initially, it is expected that services will be degraded, restricted, or even completely curtailed to some users in favor of high priority critical command and control users. The quality of service during various levels of stress can also be expected to be far different than that provided during the day-to-day pre-war environment. Lower data rates and longer delays can be expected. During times of stress, limited interconnect assets may make it necessary to employ a vastly different set of interconnect media than that which is used for day-to-day DCS data system services. To assure an appropriate allocation of reconstitution resources, the minimum essential requirements for each user must be understood. Then a cohesive hierarchical arrangement of preassigned restoration priorities to both the end users and the interconnecting circuits must be established. This should be done both internally to the DCS data system and externally within the environment that surrounds the DCS data system. These are some of the procedural considerations which must be addressed as key elements of overall reconstitution plans.

1.3 Scope

Reconstitution planning can be viewed from several different perspectives and levels. There are two distinct levels of planning: what and how. The first calls for creation of an overall reconstitution strategy that primarily consists of a framework identifying multiple areas that must be addressed to define the conceptual questions regarding "What?" must be done to achieve an acceptable level of restored services for each environmental stress level. Each of these multiple areas may be further broken down into individual interrelated plans that address specific areas of concern. The second level of planning addresses the question of "How does the community accomplish reconstitution?", This dimension can be thought

of as the development of a series of plans that address reconstitution employment strategy. Care must be taken not to jump into the second level solution strategies without first having established an approved Level One planning framework. A community level understanding of the roles and responsibilities of all interested parties will create the harmonious environment necessary to implement any level two employment strategies.

This document primarily addresses potential DCS data system reconstitution interconnect technology and points out some reconstitution employment strategies that must be considered when developing reconstitution plans. As such, we address how the DCS data system can reconstitute within its own areas of responsibility and the requirement to integrate DCS data system reconstitution plans into the local, national, and international arenas. Given the key DCS data system elements identified in Paragraph 1.1, this document focuses primarily on the interconnect environment. The other two key elements are addressed only peripherally and will need to be developed fully to provide the proper balance for the creation of a total reconstitution strategy.

This examination of reconstitution concepts is based on the assumptions that:

1. A formal message system, replacing existing AUTODIN services, will use DDN as a packet-switched transport medium

2. End-to-end encryption (E^3) technology will have been fielded

3. The majority of the related DCS components will employ digital technology for voice and data switching and transmission services

4. Commercial assets may be used (with prior arrangements) when needed

5. The typical distances and data rates are as shown for each of the access areas:

ACCESS AREAS	DISTANCE	DATA RATE
Subscriber Area	Up to 10 miles	Up to 9.6 Kbps
Access Area	10-100 miles	Up to 56 Kbps
Backbone Network Area	50-3000 miles	56 Kbps

The approach taken during the development of this document includes: 1) a review of existing documents on DCS data system and available documents relating to the reconstitution of telecommunication services for the DCS and other large-scale commercial systems; 2) an analysis and identification of the critical components of DCS data system; and 3) the evaluation of potential existing or emerging interconnect technologies which could be used for DCS data system reconstitution. From this information, we provide a comparative analysis of potentially available media for subscriber, access, and backbone interconnect support within the DCS data system. Once these potential media sources are determined, supporting employment concepts, including application of these technological capabilities,

are identified. When it comes to the employment of available interconnect media, it cannot be thought of as an either/or situation, rather it boils down to the successful application of whatever media are available during a given level of stress. These points are developed further in the remainder of this document.

1.4 References

1. Bartholome, P. J. and Vogt, I.M., "COMET - A New Meteor-Burst System Incorporating ARQ and Diversity Reception," IEEE Transactions on Communications, Vol. COM-16, pp 268-278, April 1968.

2. BLACKER Interface Control Document (ICD).

3. Briefing by RCA on ACTS, 20 June 1986.

4. Brown, D.W., "A Physical Meteor-Burst Propagation Model and Some Significant Results for Communication System Design," IEEE Journal on Selected Areas in Communication, Vol. SAC-3, No. 5, pp 745-755, September 1985.

5. Chakraborty, D., Constraints on Ku-band Continental Satellite Network Design, IEEE Communications Magazine, Vol. 24, No. 8, August 1986, pp 33-43.

6. CSC-TG-005, Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria (see Reference 18 below), Version 1, 31 July 1987.

7. CSC/GTE/BAH Report, MILSATCOM Network Interoperability and Control (U), SECRET, September 1985, (Contact: Mr. Serafino, C4S/A320)

8. CSC/GTE/BAH Report, MILSATCOM Restoral/Reconstitution (U), SECRET, October 1985, (Contact: Mr. Serafino, C4S/A320)

9. DCA Circular 310-70-1, DCS Systems Control, Vol. I, Policy and Responsibilities, Draft 6 February 1986.

10. DCA Circular 310-70-1, DCS Systems Control, Vol. II, Operational Procedures TCF/PTF/MTC's, August 1986.

11. Defense Data Network Evolution of Security Services: 1986-1992, 24 November 1985, Mitre Report.

12. Defense Data Network (DDN) PMO DF, "Use of C/30 in Tactical Environment," B101Q226-86, 26 September 1987.

13. Defense Data Network (DDN) Program Plan (Current), 1982.

14. Defense Data Network (DDN) Program Plan (Proposed), 1986, Mitre Report.

15. Defense Data Network Subscriber Guide to Security Services 1986-1992, 30 September 1986, Mitre Report.

16. Defense Data Network (DDN) System Description, January 1984, Mitre Report.

17. Defense Data Network (DDN) X.25 Host Interface Specification, December 1983.

18. DoD 5200.28STD, Department of Defense Trusted Computer System Evaluation Criteria (Supercedes CSC-STD-001-83, dtd 15 August 1983), December 1985.

19. Executive Order No. 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions," 3 April 1984.

20. Fidelman, Miles R., Herman, James G., and Baum, Michael S., "Survivability of the Defense Data Network," Signal Magazine, May 1986.

21. Fifer, W.C. and Bruno, F.J., "The Low-Cost Packet Radio," Proceedings of the IEEE, Vol. 75, No. 1, January 1987, pp 33-42.

22. Functional Requirements Document for the I-S/A AMPE, 1 April 1983.

23. Griebenow, Allen, "VSAT Implementation from the Buyer's Perspective," Telecommunications, June 1987, pp 44 et seq.

24. GTE Report, IAS/DSN Interface (IDI) Specifications, DSN SETA Task 85-10.

25. GTE Report, IAS/Digital Patching and Access System (DPAS)/Digital Access and Cross-Connect System (DACS) Analysis, DSN SETA Task 85-10.

26. GTE Report, System Concept of IDS Restoral of Services via Non-DoD Networks, DSN SETA Task 85-11.

27. Hahn, J.J., and Stolle, D.M., "Packet Radio Routing Algorithms: A Survey," IEEE Communications Magazine, Vol. 22, No. 11, November 1984, pp. 41-47.

28. Huerwicz, Mike, "Slower Modems Still Successful: Buyers Guide," Network World, Vol. 5, No. 6, 8 February 1988.

29. IEEE Journal on Selected Areas in Communications, Vol. SAC-3, No. 1, January 1985. Special Issue on Broadcasting Satellites.

30. IEEE Journal on Selected Areas in Communications, Vol. SAC-5, No. 4, May 1987. Special Issue on Satellite Communications Toward the Year 2000.

31. Ince, A.N., "Spatial Properties of Meteor-Burst Propagation," IEEE Transactions on Communications, Vol. COM-28, No. 6, pp 841-849, June 1980.

32. Integrated AUTODIN System Architecture (IASA) Report (Part 3), September 1984.

33. Integrated AUTODIN System (IAS) Interoperability and Integration, GTE Task 85-10, 29 January 1986.

34. Interface Control Document for the I-S/A AMPE, 1 April 1983.

35. Internation Organization for Standardization, "Information Processing Systems -- Open Systems Interconnection Reference Model -- Part 2: Security Architecture," Draft International Standard ISO/DIS 7498-2, 18 June 1987.

36. Inter-Service/Agency Automated Message Processing Exchange (I-S/A AMPE), Management Engineering Plan.

37. Jacobsmeyer, J. M., "Message Waiting Time Performance for Meteor-Scatter Communication Systems," IEEE Transactions on Communications, to be published.

38. Leiner, B., Cole, R., Postel, J., Mills, D., "The DARPA Internet Protocol Suite," IEEE Communications Magazine, Vol. 23, No. 3, March 1985, pp. 29-34.

39. Li, V.O.K., "Multiple Access Communications Networks," IEEE Communications Magazine, Vol. 25, No. 6, June 1987, pp. 41-47.

40. Lyon, David L., Personal Computer Communications via Ku-band Small-Earth Terminal Stations, IEEE Journal on Selected Areas in Communications, Vol. SAC-3, No. 3, May 1985, pp 440-448.

41. Messeh, Adel I., DDN Reconstitution Concept of Operations, MTR-85-00186, DCA Contract # F19628-84-C-0001, September 1985.

42. MIL-STD-1777, Internet Protocol (IP) Specification.

43. MIL-STD-1778, Transmission Control Protocol (TCP) Specification.

44. MITRE Technical Report, Defense Communications System Integrated Data Services, May 1986, MRT-86W0088.

45. MITRE Technical Report, Defense Data Network Survivability and Endurance, Dept 1985, MTR-85WA00181.

46. National Security Decision Directive Number 47 (NSDD-47), Emergency Mobilization Preparedness, 1983.

47. National Security Decision Directive Number 97 (NSDD-97) (FOUO Version), National Security Telecommunications Policy, 3 August 1983.

48. Parker, Edwin B., Future Perspective on Satellite Communications, Telecommunications, August 1987, pp 47 et seq.

49. Proceedings of the IEEE, Vol. 172, No. 11, November 1984. Special Issue on Satellite Communication Networks.

50. Public Notice 2626, "Petition for Rulemaking for the National Security Emergency Preparedness Telecommunications Service Priority System filed by the Secretary of Defense (RM-5834)," 3 April 1987.

51. RFC 904, *Exterior Gateway Protocol (EGP) Specification.*

52. Sparta Report, Department of Defense Gateway Architecture and Functional Requirements, 22 December 1985, Contract No. DCA100-84-C-0085.

53. Sugar, G.R., "Radio Propagation by Reflection from Meteor Trails," Proceedings of IEEE, Vol. 52, pp 116-136, February 1964.

54. Tobagi, F.A., Binder, R., and Leiner, B., "Packet Radio and Satellite Networks," IEEE Communications Magazine, Vol. 22, No. 11, November 1984, pp. 24-32.

55. Voydock, V.L. and Kent, S.T., "Security Mechanisms in High-Level Network Protocols," ACM Computing Surveys, Vol. 15, No. 2, June 1983, pp 135-171.

56. "VSAT Boasts Net Control, 4 Ports," Network World, 15 February 1988, p 23.

57. Worldwide Digital System Architecture (WWDSA) Final Report, 1981.

58. WWDSA, System Control for the WWDSA, PSI-83-C-0036-007, March 1984.

1.5 Document Organization

Section 2: Includes a discussion of the DCS environment pre- and post- stress; an identification of DCS data system elements; a delineation of reconstitution responsibilities for the related DCS components; and a discussion of DCS data system security aspects for reconstitution.

Section 3: Identifies and discusses existing or emerging technologies that could be used for DCS data system interconnect service, a survey and evaluation of techniques and technology to be employed during various levels of stress.

Section 4: Provides a summary and comparative analysis of the interconnect technologies discussed in Section 3 and some recommendations for employment during defined levels of stress.

Section 5: Provides recommended strategy for development and acquisition of pre-planned interconnect services and the identification of interface equipment required for implementation of DCS data system reconstitution plans.

Section 6: Provides a summary wrap-up of task report including recommendations to be addressed during the development of the other two key elements of DCS data system reconstitution planning.

Appendix A: Contains a limited glossary of terms.

Appendix B: Contains a list of applicable acronyms.

Appendix C: Identifies Levels of Stress as identified in the DDN Program Plan and in the National Security Emergency Preparedness Telecommunications Service Priority System.

SECTION 2 - Understanding the IDS

2.1 Systems Concept

The word "system" is one we talk about often; however, most of us do not concern ourselves with the details of the total system, but tend only to be interested in that portion which appears ***visible*** to us in our everyday life. When addressing reconstitution planning, one must consider the details of the total system. Webster defines a system as "a set or arrangement of things so related as to form a whole." The point to emphasize here is the interrelationship of the working parts which influences the satisfactory objective of the whole. The simple design of a three legged milk stool, illustrated in Figure 2-1, has four distinct physical parts: three identical legs and a seat. If the seat or any leg were missing, the stool would not function as it was designed. So it is with the large scale communication *systems* employed to serve the needs of their customers. A communication system is made up of many active components. These components can be divided into dependent and independent categories. Another way of expressing this is that some components are totally within the defined system and others are a subset of the environment in which the defined system exists. A data terminal is an example of an independent component, whereas the supporting interconnects are a good example of a component that is shared and dependent on the environment of a larger system. In the early days of the developing communications industry, each instrument required its own connectivity. Those days are long past. Technology now absorbs many customers combining their requirements into multichannel systems transmitted over links using a common transmission medium.

Hence, it can be stated that a system can have shared components with a larger system. The definition of ***System*** allows us to build a hierarchy of systems with each system being a subsystem of a larger one.

2.2 Environmental Relationships

The DCS data network system is a common-user switched system that can be viewed as a value-added data exchange server that builds upon raw transmission facilities and services to provide data exchange services to the system users, operators, and managers. As such, the DCS data network is a world-wide subnetwork of the Defense Communications System (DCS). It is necessary to examine this relationship prior to getting into reconstitution planning for the DCS data network. The DCS is rapidly transitioning toward an integrated digital system with an interrelated hierarchy of subsystems. The DCS consists of a series of layered networks/subsystems sharing common components to provide required customer services. These systems and services being provided by the elements of the DCS may be viewed from several different perspectives. From a user's perspective, service requirements

are simply stated on a from-to basis with a specified data rate and required quantity of circuits. When service is provided, everything between one subscriber's terminal equipment and the distant end becomes totally transparent to the users. However, as principal providers of that customer service, it is necessary for the DCS data network/DDN planning community to understand the complexity and interrelationships of the sibling networks and subsystems located within this transparent area, identified as raw transmission facilities and services. An examination of this hierarchy reveals that two major independent networks co-exist within the DCS: the Defense Switched Network (DSN), which is designed to handle primarily voice traffic, and the Defense Data Network (DDN), a principal component of the DCS data network, which primarily handles data traffic. These sibling networks are both provided interconnectivity via the same physical facilities, government-owned or leased transmission systems. The DSN and DDN have developed network topologies based on end-to-end defined customer service requirements. The government-owned or leased transmission facilities provide the physical paths for the desired electrical connectivity specified by the DSN or DDN traffic analysts and topological designers. Figure 2-2 shows this hierarchy of complimentary DCS components. Figure 2-3 shows the physical relationships at a representative composite DCS site. Since reconstitution depends upon the reality of the physical relationships, a basic understanding of these DCS elements and their interrelationships is necessary prior to development of specific reconstitution plans for any networks or subsystems of the DCS. Additionally, while the DCS data network and DSN share interdependent elements of a larger system (DCS), terminology and definitions are an integral part of the requirement to understand the differing perspectives. Words like *user, customer, subscriber, end-to-end, network, and even system have differing meanings*

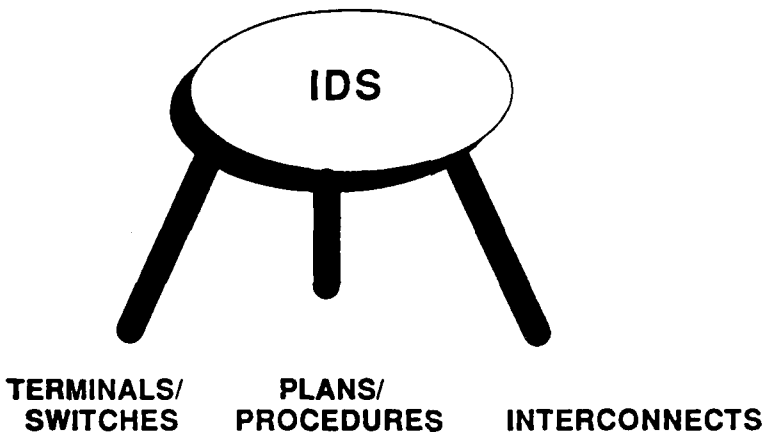


Figure 2-1. Key Elements for Data Transmission

depending on which program you are discussing. When you start mixing elements of major programs this sensitivity becomes even more acute.

2.3 IDS Network Description

With these basic relationships in mind, Figures 2-4 and 2-5 depict a generic (FY92) systems view of the major DCS data services sub-networks (MILNET, DISNET). It must be remembered that Figures 2-4 and 2-5 represent a logical connectivity perspective of the DDN subelements of the DCS rather than the physical relationship of the DCS components

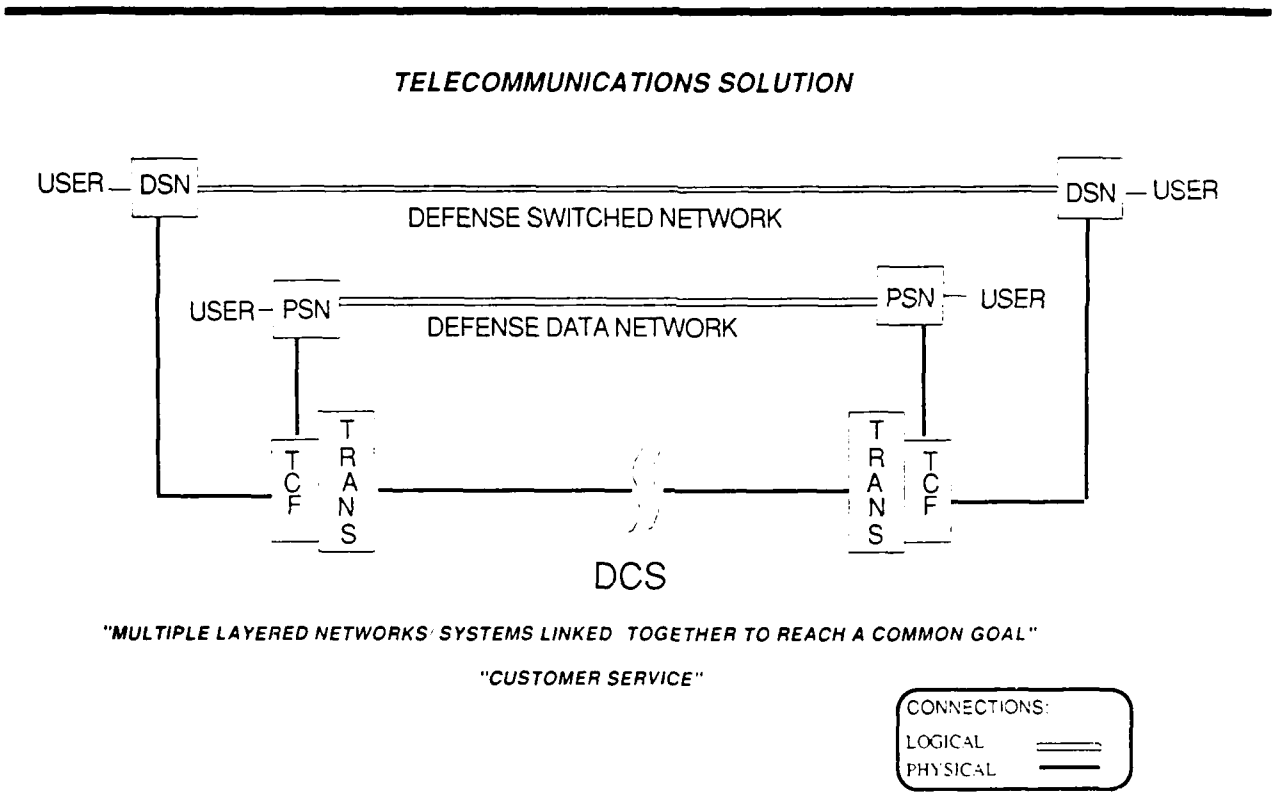


Figure 2-2. DCS Functional Relationships

shown in Figure 2-2. From a DCS data services network perspective, they have several identifiable components: the subscriber area, the access area, and the backbone network.

2.3.1 Subscriber Area

The subscriber area is defined as customer premises terminal equipment, consisting of hardware and facilities (i.e., hosts, gateways, terminals, end-to end encryption (E^3 devices, and LANs and local area interconnect systems). These local area interconnect facilities are a functional responsibility of the subscriber community. Generally, they are provided by the cable and radio distribution plant of the supporting Post, Camp, or Station.

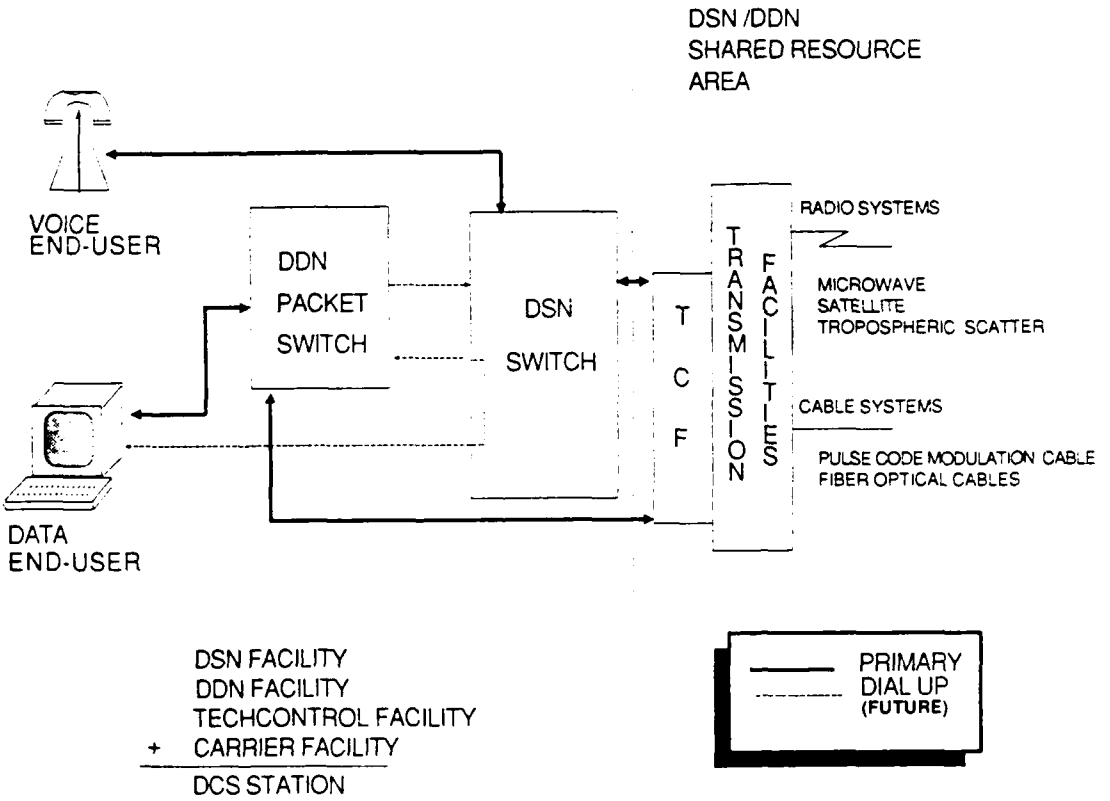
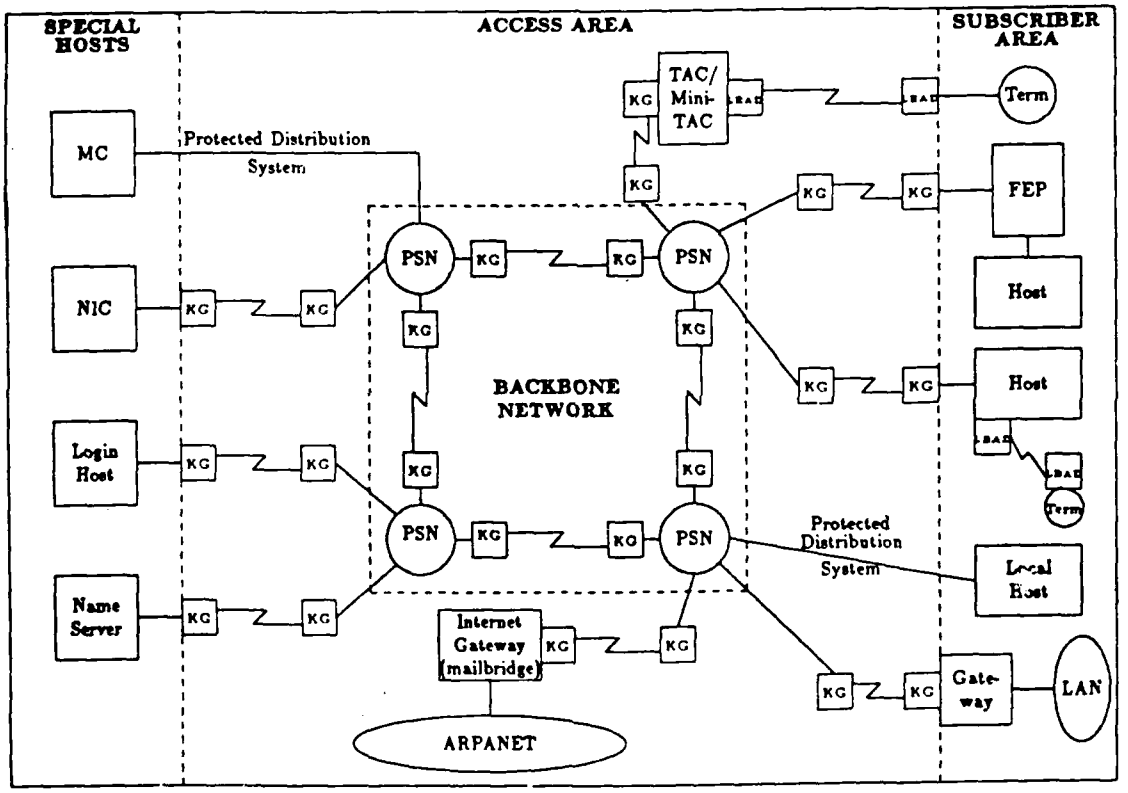


Figure 2-3. Representative DCS Station Configuration

2.3.2 Access Area

The access area is that shared area that contains the communications connectivity and interface facilities which connects the supported subscriber area equipment with the supporting packet switch node(s). This area may include the encryption devices required to provide link and/or host-to-host security services. Generally, the interconnect services are provided to the government-owned or leased bulk transmission facilities which are the interconnect links between the terminal/switch locations.



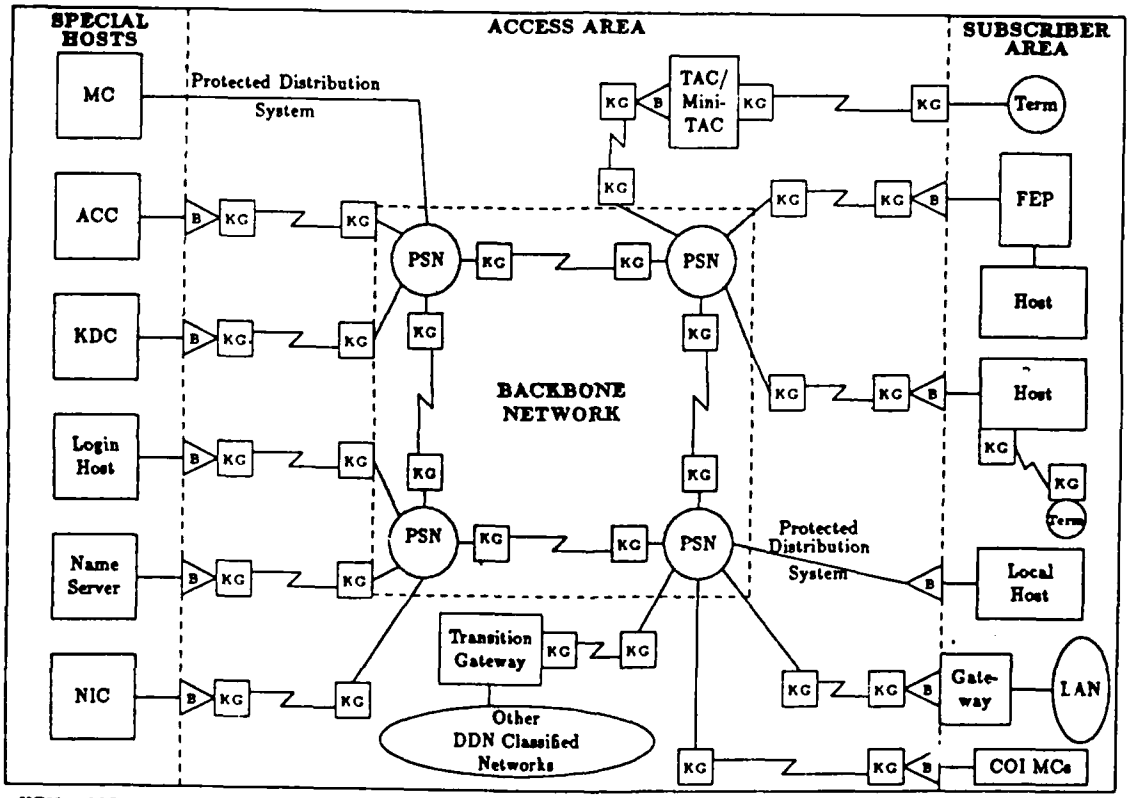
KEY: MC = Monitoring Center
NIC = Network Information Center
PSN = Packet Switching Node
TAC = Terminal Access Controller
Term = Terminal
FEP = Front-End Processor
LAN = Local Area Network
LEAD = Low Cost Encryption and Authentication Device
KG = Link Encryption Device (KG-84A)

(Extracted from Draft DDN Program Plan, 1986)

Figure 2-4. Generic View of MILNET (FY92)

2.3.3 Backbone Area

The backbone network consists of packet switching nodes, link encryption devices, control facilities (i.e., monitoring centers, key distribution centers, etc), and an interconnecting array of multi-media 56 kbps trunk circuits based on pre-determined requirements resulting from an analysis of user relationships and a documented topological design. These interconnect services are provided by long haul government-owned or leased transmission facilities which are the physical interconnecting paths between the switch nodal locations.



KEY: MC = Monitoring Center
ACC = Access Control Center
KDC = Key Distribution Center
PSN = Packet Switching Node
NIC = Network Information Center
TAC = Terminal Access Controller
Term = Terminal
FEP = Front-End Processor
B = BLACKER Front End (BFE)
LAN = Local Area Network
KG = Link Encryption Device (KG-84A)
Note: Transition gateway includes BFE

(Extracted from Draft DDN Program Plan, 1986)

Figure 2-5. Generic View of DISNET (FY92)

2.4 IDS Reconstitution Requirement Concepts

These components, coupled with the special hosts required for network operation and control, each need to be addressed as system components during the creation and development of any reconstitution concepts relating to equipment technology application or deployment/employment planning. Reconstitution planning requires that the physical realities of these components be closely examined rather than the generic drawings shown in Figures 2-4 and 2-5.

When addressing reconstitution, it is necessary to focus on the critical elements of DCS data network. A reconstitution planner must start with the question "What is it that needs to be reconstituted, when considered from the perspective of critical elements?" The matrix contained in Figure 2-6 divides these identifiable components of DCS data network into three major categories: Facilities, Interconnects, and Plans and Procedures. The Facilities include several distinct type of equipment configurations: 1) packet switches, 2) special hosts, 3) TACs and gateways, and 4) subscriber/host terminals. The plans and procedures must address network operations across the entire spectrum of the peace-to-post war

RECONSTITUTE

?

DDN COMPONENT	FACILITIES	INTERCONNECTS	PROCEDURES
BACKBONE NETWORK	- PACKET SWITCHES - SPECIAL HOSTS	INTERSWITCH TRUNKS	DCAC NETWORK OPLANS
ACCESS AREA	TACs GATEWAYS	ACCESS LINES	DCAC OPERATING PROCEDURES
SUBSCRIBER AREA	HOST LAN GATEWAYS TERMINALS	SUBSCRIBER LOOPS	MILDEP/USER LOCAL SOPs

Figure 2-6. DCS Data Network Component Elements

environment. The data switch nodes and system operating plans and procedures are unique to the DCS data network; however, the interconnects are shared components within the much larger DCS. Responsibility for local area subscriber/host systems rests with the user community and does not extend into the DCS data network. **The primary focus of DCS data network reconstitution must be on development of a replaceable packet switch capability, the development of appropriate restoration plans and procedures, and on the application of interconnect technologies that can ensure a functioning DCS data network that meets the needs of surviving users.** The existence of reconstitutable switch nodes and the requisite network restoration plans and procedures are considered internal to the DCS data network ***System*** and are not fully developed in this report. As pointed out in Section 1, this document primarily addresses potential interconnect technologies and outlines developmental strategy considerations.

As shown in Figure 2-6, interconnect facilities are divided into two categories: access area and backbone. The interconnect facilities within the access area can be further subdivided into local and subscriber connections. These facilities are usually point-to-point wire lines and are generally short in distance. In the day-to-day, pre-stress environment, it is the users' responsibility to arrange for and provide local/subscriber area connectivity in conjunction with their supporting post, camp, or station communications activity. The backbone area consists of leased or government-owned, long haul carrier facilities, providing inter-nodal connectivity. These types of interconnect facilities are subject to DCS reconstitution plans, and any inter-nodal DCS data network circuit requirements must be compatible with these established plans. DCS data network interconnect circuits in each of the interconnect areas must independently justify the appropriate restoration priority level of their service requirements.

The transmission speeds supported by the DCS data network vary based on the attachment method and the physical interface standard. Basically, the DCS data network supports access speeds from 75 bps to 56 kbps. Other access speeds are supported to: 1) provide for tactical/strategic interoperability, and 2) adapt to support emerging user requirements for faster data exchange rates. For purposes of this effort, DCS data network interconnect requirements are assumed to have the following general characteristics:

ACCESS AREAS	DISTANCE	DATA RATE
Subscriber Area	Up to 10 miles	Up to 9.6 kbps
Access Area	10-100 miles	Up to 56 kbps
Backbone Network Area	50-3000 miles	56 kbps

2.4.1 Interconnect Reconstitution Considerations

Commercial and government-owned transmission and communication facilities are used to provide interconnecting communication links and services between the DCS data network terminal and switch nodal components located in the subscriber, access, and backbone areas. These interconnecting facilities within CONUS are subject to established restoration priorities in accordance with the rules and regulations identified in the National Security Emergency Preparedness (NSEP) Telecommunications Service Priority (TSP) System. All DoD service requirements are satisfied within the scope of this system. This system provides a single, integrated, peacetime and wartime telecommunications service priority system as promulgated by the Federal Communications Commission (FCC) and the Executive Office of the President (EOP) and is administered by the Director of DCA through the National Communication System (NCS). This system includes the provisioning of initial service during peacetime as well as restoration of service for three defined levels of stress (See Appendix C). It encompasses inter-city public switched and private line services, and non inter-city private lines. The structure of the priority levels within the NSEP TSP System has been designed to accommodate technological evolution toward all-digital transmission, signaling, and switching. It also allows for assigning priority levels to services and even to users, rather than only to dedicated circuits.

In the overseas areas, the primary source of DCS communications connectivity is U.S. Government-owned cable and microwave systems supplemented by some host nation systems. The development and employment of reconstitution plans for these resources are controlled by the applicable theater commander, addressed in existing contingency plans, executed by the supporting DCA field office, and carried out by the appropriate MILDEP. Limited reconstitution priority plans also exist within the structure of the host nation telecommunication systems similar to the NSEP TSP system for restoration and reconstitution; however, these vary widely from country to country. Use of host nation civil or military systems is not under the control or direction of the theater commander and, therefore, cannot be assured unless extensive pre-war agreements are firmly in place. Any plans to employ these interconnect facilities for reconstitution purposes must be closely coordinated and examined prior to dissemination. The DDN Program Plan identifies a different set of stress levels than that used by the NSEP TSP system. These stress levels are identified in Appendix C. Coordination is required to resolve the differences in the definitions of the various stress levels.

2.4.2 Network Interconnect Analysis

A review and understanding of the identifiable components of the DCS data network and the environmental relationships outlined above reveals that the three areas of concentration for reconstitution of DCS data network services must be considered to ensure a true ***Reconstitution Plan***. In the area of communications interconnects there is a known spectrum of possible types of switched and transmission/multiplex system interfaces that could be used to satisfy DCS data network requirements. Two major categories of technology are employed to provide interconnect services: 1) radio systems (HF, tropo, microwave, satellite) and 2) cable systems (metallic, fiber optic, coaxial).

Sections 3 and 4 of this document focus on the types of interconnect facilities that exist in the inventory and their potential application for DCS data network use during times of stress or reconstitution. Some of the technologies discussed extensively are radio systems (HF, Satellite, Meteor Burst, and Packet Radio) and cable systems for use in subscriber or access area connectivity applications. Section 5 addresses some application considerations in a generic form using a line-of-sight (LOS) radio example. Section 6 provides a framework for developing specific strategies and a roadmap for reconstitution planners.

2.5 Security Requirements

Security requirements are generally discussed in terms of protection from compromise, protection of data integrity, protection from denial of service, and access control. Compromise is disclosure to unauthorized entities; on a network, compromise takes two forms: the content of the messages on the network and the message traffic flow. Data integrity on a network exists when the data received is the same as that sent; integrity can be lost accidentally or with malicious intent. Denial of service is the condition wherein a network does not have the capability to execute all of its prescribed functions or services. Access control is identification of system access, authentication of the access, and control of access to ensure protection from compromise, protection of data integrity, and protection from denial of service.

The DDN security requirements are described in Defense Data Network Evolution of Security Services (Reference 11) and Defense Data Network Subscriber Guide to Security Services (Reference 15). In addition, discussion of security on a network is available in the Open Systems Interconnection Reference Model Part 2: Security Architecture (Reference 35) and the Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria (Reference 6). The following paragraphs describe what each of these documents contributes to security requirements for reconstitution.

1. The Defense Data Network Evolution of Security Services, Reference 11, is *concerned with providing the following security services:*

* Data Confidentiality
    - Mandatory Confidentiality
    - Discretionary Confidentiality
    - Traffic-Flow Confidentiality
* Data Integrity
* Identification, Authentication, and Access Control
* Data Origin Authentication
* Non-Repudiation
* Availability.

Trunk and access lines, both Host and TAC, will employ KG-84As for link encryption on dedicated DDN lines. The reconfiguration discussion of dial up backup trunking, use of Digital Switched Network (DSN), and use of public Integrated Services Digital Networks (ISDNs) does not include security requirements.

2. The Defense Data Network Subscriber Guide to Security Services, Reference 15, identifies the following list of security services:

    * Data Confidentiality
        - Mandatory Confidentiality
        - Discretionary Confidentiality
        - Traffic-Flow Confidentiality
    * Data Integrity
    * Availability
    * Identification, Authentication, and Access Control
        - Identification, Authentication, and Access Control
        - Data Origin Authentication
        - Non-Repudiation.

    KG-84As for link encryption will provide traffic flow confidentiality for dedicated lines. End-to-end encryption (E^3) will enforce mandatory and discretionary confidentiality; support data integrity; and provide identification, authentication, and access control.

3. The draft Open Systems Interconnection Reference Model Part 2: Security Architecture, Reference 35, recommends security services to be provided at specific levels of the Reference Model as shown in Figure 2.7.

Security Service	ISO-OSI Reference Model Layers
Authentication	
Peer Entity Authentication	3 4 6[2] 7
Data Origin Authentication	3 4 6[2] 7
Access Control	3 4 7
Data Confidentiality	
Connection Confidentiality	1 2 3 4 6 7
Connectionless Confidentiality	2 3 4 6 7
Selective Field Confidentiality	6 7
Traffic Flow Confidentiality	1 3 6 7
Data Integrity	
Connection Integrity with Recovery	4 6[2] 7
Connection Integrity without Recovery	3 4 6[2] 7
Selective Field Connection Integrity	6[2] 7
Connectionless Integrity	3 4 6[2] 7
Selective Field Connectionless Integrity	6[2] 7
Non-Repudiation	
Non-Repudiation with Proof of Origin	6[2] 7
Non-Repudiation with Proof of Delivery	6[2] 7

WHERE:

7 = Application Layer
6 = Presentation Layer
5 = Session Layer
4 = Transport Layer
3 = Network Layer
2 = Data Link Layer
1 = Physical Layer

Figure 2-7. Security Services vs ISO-OSI Reference Model Layers

[2]The Presentation Layer may support the provision of these security services by the application layer to the application process.

4. The Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, Reference 6, specifically exempts itself from interpreting for complexly composed networks, such as DDN.

We acknowledge the caution exhibited in the aforementioned first two documents by not specifying inflexible reconstitution security requirements. In summary, using the list of security services identified in the DDN Subscriber Guide to Security Services, Figure 2-8 shows the desired security services and, given the ISO-OSI recommendations, the appropriate layers at which to apply them.

The actual security requirements during reconstitution of the network must be a tradeoff available to the users. Timeliness of the messages, sensitivity of the messages, necessity of the messages, and availability of resources will all combine to establish different security requirements for reconstitution. The security paragraphs for each of the technologies in Section 3 identify the specific security concerns and solutions that applies to that technology.

Required Security Services	Equipment Location
Data Confidentiality	
Mandatory Confidentiality	E^3
Discretionary Confidentiality	E^3
Traffic-Flow Confidentiality	Link
Data Integrity	E^3
Availability	Switches and Circuits
Identification, Authentication, and Access Control	
Identification, Authentication	E^3 and Switches
Access Control	Switches
Data Origin Authentication	E^3
Non-Repudiation	E^3

Figure 2-8. Locations of Security Solutions

This Page Left Blank Intentionally.

SECTION 3 - Technology Concepts for IDS Reconstitution Interconnects

3.1 Introduction to the Technology Survey

The technology survey conducted for the DCS data services reconstitution focuses on those technologies that will most likely exist in the environment and would potentially be available to satisfy the interconnect requirements of the DCS data services reconstitution in the near term (1990s). Some of the technology is available today, some is under development, and some will have to be developed or enhanced to meet the specific needs of the DCS data services. In addition to the technology requirements of the DCS data services reconstitution, cost is another major consideration in the survey of potential interconnect capabilities. The preferred method of interconnect is through land lines, as provided in the pre-war environment. However, it is recognized that these facilities will at the very least suffer collateral damage and may not be available for use in the post-attack period. Of the wide-ranging, promising and presently available technology alternatives, those that appear most likely to take advantage of off-the-shelf components and integrate easily with current and future DCS data services reconstitution efforts are considered. The technologies addressed include packet radio, high frequency radio, meteor burst, very small aperture terminals (VSAT), and dial-up switched service.

3.1.1 Packet Radio

Packet radio technology is the application of packet switching techniques to the radio transmission medium. Packet radio networks (PRNETs) provide packet switching services over a wide geographic area to mobile users (hosts and terminals) and fixed users not readily accessible through hard-wire facilities. In the context of the IDS, PRNETs will serve the subscriber area, providing communications among hosts and users and access to the DDN or other packet switched networks through designated gateways.

While PRNETs perform the same functions as hard-wired packet switching systems, they are more complex to implement because of limitations imposed by the transmission medium. Apart from propagation considerations (e.g., obstruction losses, multipath fading) there is the problem of contention for the transmission channel, similar to the contention problems experienced in local area networks (LANs). Flow control and routing are other problem areas, particularly in a mobile radio network. Much development work has been undertaken in the PRNET area, particularly by the Defense Advanced Research Projects Agency (DARPA).

3.1.1.1 Packet Radio Architectures

There are two basic architectures to consider: centralized and decentralized. Centralized architectures comprise one centrally located broadcast/control facility (called a station) through which all the network packet radio units (PRUs) intercommunicate (repeaters may be used to provide access to PRUs outside the coverage area of the station). The station provides the switching, routing and control functions for the network. (Multiple station networks have also been considered in which stations control different parts of the network, increasing network survivability.) In decentralized (more commonly called stationless) architectures, switching, routing and control functions are distributed among all the network PRUs. The centralized architectures tend to have greater network throughputs and more efficient routing (i.e., use shorter routes). However, they are less survivable in that loss of the station cripples the network.

3.1.1.2 Characteristics of the Transmission Medium

In selecting a frequency for a PRNET, the designer is faced with various tradeoffs. On the one hand, a high frequency is desirable in order to permit a large bandwidth, which translates into higher data rates and allows use of spread spectrum techniques. On the other hand, path attenuation (free space loss, obstruction losses, and losses due to rain) increases nonlinearly with frequency, which means less range for an equal transmit level. In addition, losses due to obstructions (buildings, trees, etc.) also increase with frequency. As indicated in Reference 54, a practical upper limit on PRNET frequencies is 10 GHz.

A major propagation problem for radio systems, particularly mobile systems, is multipath, which is caused by reflections of the original signal arriving at a receiver. These reflections arrive at the receiver delayed with respect to the direct signal because their path length is longer. The result is superposition of the signals. If the delay is on the order of a symbol duration or greater, the multipath causes intersymbol interference that results in errors. A good way to combat the effects of multipath is to use spread spectrum modulation techniques, either direct sequence or frequency hopping.

Spread spectrum modulation provides bandwidth expansion and multiple access[2]. The bandwidth expansion n, which is typically one or two orders of magnitude, relative to the bandwidth of the information signal, suppresses intersymbol interference. It also provides protection against jamming, a signal-to-noise ratio improvement equal to 10 $\log(n)$, and allows different users and systems to coexist in the same frequency band. For these reasons,

---

2. Bandwidth expansion is accomplished by modulating the information signal with a high rate (equal to the expansion factor), pseudorandom spreading waveform in the case of direct sequence, or changing the carrier frequency pseudorandomly across a wide bandwidth in the case of frequency hopping. To receive a signal, a receiver must know the pseudorandom spreading or frequency hopping code and be able to synchronize with the spreading or frequency hopping waveform. The pseudorandom code provides the multiple access, or coexistence, capability.

both direct sequence and frequency hopping spread spectrum techniques are being used in experimental PRNETs.

3.1.1.3 Protocols

A multitude of protocols are used in PRNETS: the low-level protocols used to transmit packets among PRUs and the higher-level network and internet protocols that provide the means for hosts to access the network and provide an end-to-end communication capability. The focus of the following discussion is the protocols peculiar to PRNETS: channel access protocols, acknowledgement procedures, and network management and monitoring functions necessary to control the operation of PRNETS. (Reference 38 describes the DARPA internet protocol suite that is common to all packet switching networks.)

3.1.1.3.1 Channel Access Protocols

Channel access protocols define how network PRUs will use the communication channel. In particular, the problem addressed by channel protocols is the self-interference that results when two or more PRUs transmit packets such that they collide at a receiving PRU, destroying the colliding packets. The following discussion focuses on spread spectrum signaling because the experimental work being done point to it as the most likely candidate for use in the IDS.

A property of spread spectrum that reduces the self-interference problem is known as capture. Capture means that a receiver will successfully receive a signal that it has locked onto despite the presence of interfering signals. There are two windows of vulnerability during which the capture effect does not operate, leading to loss of the packet. One is during the preamble phase, in which the receiver is trying to synchronize with the received signal; and the other is when an interfering packet arrives a small fraction of a symbol duration after the desired packet (causing intersymbol interference).

To reduce these vulnerabilities, orthogonal pseudorandom code addresses can be assigned to network PRUs. By so doing, only packets destined for the same receiver can interfere with each other. Furthermore, a form of carrier sensing can be incorporated in which a PRU listens to the code of its intended destination. If the PRU's receiver locks onto a packet on that code, it inhibits transmission of its packet on the assumption that the intended receiver has also locked onto that packet.

3.1.1.3.2 Packet Acknowledgements

Acknowledgements are needed to notify the transmitting PRU that a packet has been received successfully, using cyclic redundancy check (CRC) codes to determine the accuracy of the received packets. Two types of acknowledgements are commonly used: hop-by-hop (link-level) and end-to-end[3]. PRUs save a copy of every transmitted packet until they

receive an acknowledgement from the next PRU.

The preferred hop-by-hop acknowledgement scheme is to return a short acknowledgement packet (know as explicit acknowledgement). While bandwidth inefficient, this scheme is less prone to interference and can be given priority which speeds up freeing of buffers.

Both types of acknowledgements are needed in a network. If a source PRU does not receive an acknowledgement packet within a certain time limit, it retransmits the packet. The hop-by-hop acknowledgement allows for retransmission of packets between intermediate nodes when failures occur, reducing end-to-end retransmissions.

3.1.1.3.3 Network Management and Routing

In PRNETs, particularly those with mobile subscribers, network topologies do not remain fixed: propagation conditions change and mobile subscribers change their locations. Thus, routing tables must change dynamically. In centralized architectures, the station collects management information and then distributes routing information to its subordinate PRUs. When there are multiple stations, the stations exchange routing information among themselves for dissemination to their area PRUs. In stationless networks, the PRUs assess local connectivity and exchange routing information with their neighbors. In either case, routing information may be out of date, so alternate routing procedures are necessary to allow PRUs to use other PRUs in case packets sent via a primary route times out.

The ARPANET uses directed broadcast routing in which the PRUs maintain their own connectivity and delay matrices. Periodically, each PRU transmits a distance vector (which contains an estimate of the minimum delay to every PRU in the network) and status information to its neighbors for use in updating routing information. Transmitted packets include the address of the destination PRU and the next enroute PRU. If the enroute PRU fails to obtain an acknowledgement from the next enroute PRU after a given number of reattempts, it tries an alternate route. While inefficient in its use of bandwidth because of the overhead caused by the exchange of routing information, this scheme is robust.

An alternate scheme is to flood route finding packets from source to destination. The destination selects the best (minimum delay) route and returns a route setup packet along the selected route. Enroute PRUs store the routing information for use in routing packets to the particular destination. Packets to that destination are thereafter sent along that route, until it fails. Alternate routes are used by enroute PRUs if repeated attempts to use the preferred PRU fail. This scheme is also robust. Its disadvantages are that the minimum delay routes may not always be selected; and since there is no congestion control, long delays could occur.

---

3. End-to-end ackno. ledgements are part of the transport protocol, such as the DoD TCP protocol.

3.1.1.4 Packet Radio Technology

Research on packet radio networks began in 1970 at the University of Hawaii, the ALOHA network. In 1973, research began on PRNETS under funding from the DARPA. This research resulted in the implementation of the DARPA PRNETs. These experimental networks have been in operation for more than 10 years for experimental purposes at Ft. Bragg, North Carolina, at SAC in Omaha, Nebraska, and in the San Francisco Bay area. Their principal aim is to provide computer communication services to fixed and mobile users.

One of the experimental efforts underway is the development of a Low Cost Packet Radio (LPR) for mobile users[5]. These radios operate in the 1.8 GHz region, use direct sequence spread spectrum modulation with variable data rates from 100 to 400 kbps, and contain a programmable digital processor. The combination of the processor and the radio frequency portion of the LPR provide the functionality of the lower three levels of the International Standards Organization (ISO) Open System Interconnection (OSI) Reference Model; that is, the physical, link, and network layers.

A packet switching applique is also under development for tactical VHF radios; namely, the SINCGARS, ARC-186, and VRC-12 radios[6]. The applique provides all the functions necessary to use the radios as the physical media for a PRNET. This VHF PRNET differs from the DARPA PRNET in more than just the frequency band used. Frequency-hopping spread spectrum is used and channel data rates are limited to 16 kbps.

There are also other experimental PRNETs in existence. The University of California has implemented a PRNET to support its automated on-line catalog system. This PRNET operates in the 2.5 GHz region using low-cost commercially available radio transceivers and standard personal computers (IBM PC-ATs). The Navy has an HF PRNET for their special applications. There is also an amateur radio PRNET.

3.1.1.5 Use of Packet Radio Technology in a Reconstitution Environment

Packet radio technology will be useful in providing packet switching services to mobile users and to fixed users for whom land lines (leased or Government-owned) are either too expensive or unavailable. PRUs deployed at DDN nodes will serve as gateways into the DDN. In a reconstitution environment, packet radios could be used to restore service to users whose access lines to their serving DDN nodes are disrupted. In cases where a DDN node is disrupted, mobile packet radios could be deployed to restore communications among local hosts/users. PRUs could also be deployed at nearby transmission nodal points to serve as gateways from PRNETs into the DDN or other packet switching networks, provided that circuits can be established to other DDN or packet switched network nodes.

---

5. Hazeltine Corporation, DARPA, and U.S. Army Communications-Electronics Command (CECOM) under Contract DAAK80-81-C-0213.
6. SRI International, ITT-A/OD, and U.S. Army Communications-Electronic Command (CECOM) under Contract No. DAAB07-85-C-K581

At the present state of development, packet radio technology is still in the experimental stage and is too expensive for commercial applications. Its use for IDS Reconstitution will become more viable when current experiments are concluded and standards are set for frequencies, signaling, channel access protocols, routing, and network management.

3.1.1.6 Security Considerations

The security requirements discussed in Paragraph 2.5 include protection from compromise, protection of data integrity, and protection from denial of service. Given that any radio signal is subject to detection, interception, and jamming (interference), special measures must be taken to mitigate these threats. Through the use of spread spectrum modulation techniques, multiple access schemes, forward error correction (FEC) schemes, transmit power level control, variable transmit data rates, and the use of data encryption devices, packet radios such as the DARPA LPR and the SINCGARS can provide a high degree of protection against jamming, interference, and compromise.

3.1.1.7 Other Considerations

Performance objectives used in the design of the DARPA LPR radios are as follows:

* Typical ranges: Line-of-sight, up to 6 miles for radios with 5 watt transmitters. Operating range could be increased by using greater transmit power, and larger/higher antennas. VHF radios will have greater operating range

* Data Rates: 100 to 400 kbps

* Operating frequency: 1.8 GHz

* Modulation technique: direct sequence spread spectrum, minimum shift keyed (MSK) chip modulation, and coherent phase shift keying (PSK) bit modulation

* Probability of correct packet detection: 95 %

* Probability of false packet detection: 10^{-6}

* Undetected bit error rate (CRC mode): 10^{-12}

* Link bit error rate: 10^{-5}.

3.1.2 Very Small Aperture Terminal

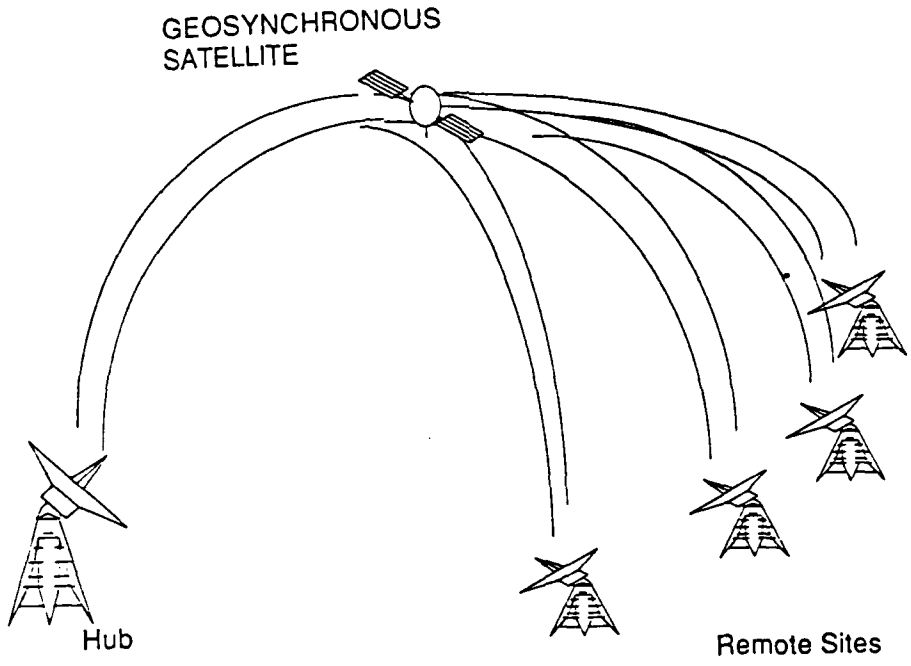
Satellite based interconnect technology has three distinct components: the land line interface, the earth terminal, and the space segment. The term VSAT, Very Small Aperture Terminal, is generally associated with a satellite communication (SATCOM) system operating in the Ku- frequency band (12-14 GHz) with communications between a fairly large earth-terminal hub (e.g., six-meter antenna) and multiple, small (hence VSAT) remote earth-terminals (e.g., 1.8-meter antennas). These low cost remote terminals (e.g., $5,000) are what has made these systems so popular. In this discussion we expand the definition of VSAT to include systems that operate at Ka-band (17-30 GHz) and receive-only systems such as used with direct broadcast satellites. C-band television, receive-only, is not considered. Some detail regarding this technology is required to understand the limitations and benefits for DCS data services reconstitution.

3.1.2.1 VSAT Architectures

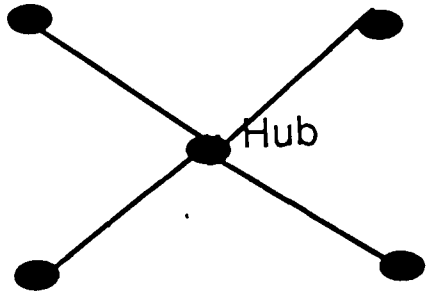
The most common VSAT architecture, shown in Figure 3-1, corresponds to a star topology with the large hub earth terminal at the center. Two-way communications can be supported between remote terminals and between the hub and remote terminals using the hub as a relay. Typical data rates supported are 2.4 to 56 kbps, depending on how the transponder in the satellite is utilized (discussed later). This architecture can also be used for receive only (i.e., direct broadcast mode where very high one-way data rates (Mbps) are possible, since the satellite transponder is dedicated to a single uplink). A second architecture is possible using only VSAT earth stations, as shown in Figure 3-2, in which any pair can communicate. Such an architecture, which corresponds to a fully connected mesh network, will support only low data rates (i.e., 75 bps to 9.6 kbps) depending on the number of users, as discussed later.

3.1.2.2 The Space Segment

Perhaps the most critical aspects of the application of VSAT resources as a reconstitution system are the availability and characteristics of the space segment assets. The time period from concept definition to operational capability of an individual spacecraft is about seven years. This rules out development and acquisition of a new spacecraft for this application. Two sets of commercial satellites could be used for a VSAT system: (1) those designed for direct broadcast operating in the Ku-band, and (2) those designed specifically for VSAT service operating in the Ku-band. Another satellite that should be considered is the NASA Advanced Communications Technology Satellite (ACTS) which was designed to operate at Ku- and Ka-bands. Finally, we should consider DoD satellites. In particular, MILSTAR, which operates at 45/20 GHz, could be considered. See References 7 and 8 for information on the use of military satellites. It is not discussed here because access to that system would fall into the category of derived service from an existing earth station, rather than the direct

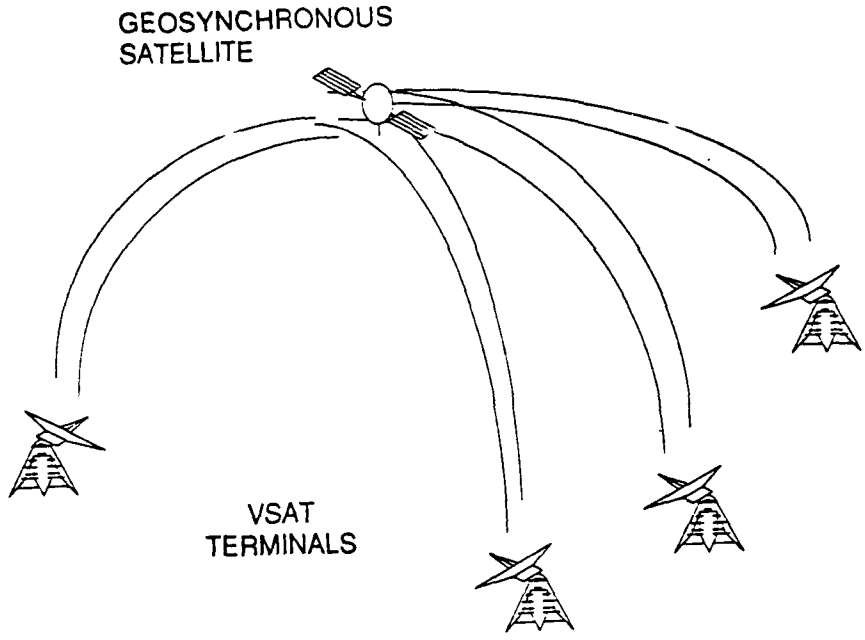


a) Physical Configuration

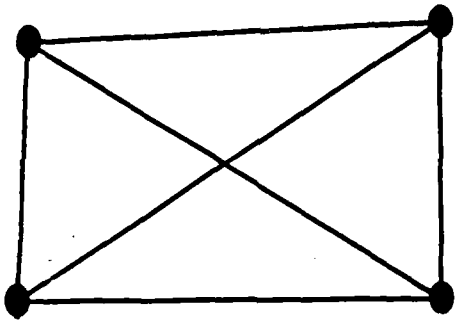


b) Equivalent Star Network

Figure 3-1. Normal VSAT Architecture



a) Physical Configuration



b) Equivalent Mesh Network

Figure 3-2. Alternate VSAT Architecture

employment of the small on-site user terminals associated with a VSAT system. A next generation DSCS is being considered that may carry a 30/20 GHz or 45/20 GHz package. This is a candidate for VSAT-type application but is not considered further due to the probability it may not be operational in the early 1990's.

The footprint associated with a spacecraft defines the specific earth coverage available. All users of this system must be located within this common footprint. The restriction of the commercial satellites which use VSAT earth stations and ACTS is that their antenna footprints are designed for servicing large metropolitan areas within CONUS, with some minor exceptions. Hence, any VSAT system used for reconstitution would be limited to CONUS locations. At this time, future growth and application of this type of interconnect technology in overseas areas is unknown and access to international or foreign satellite systems for use by U.S forces may be extremely limited.

The use of direct broadcast satellites requires a "head end," which is a large earth terminal transmitter site. Access to this large transmitter site would be controlled by EOP/NCS reconstitution plans and could be used to support national interests. It would then be possible for DoD, possibly on a shared access basis, to broadcast voice, data, and video traffic to small earth terminals anywhere in the spacecraft's coverage area (CONUS-wide, half-CONUS, one-quarter CONUS, or spot beams in CONUS).

Spacecraft designed specifically for VSAT service utilize shared transponders. Obtaining a clear channel would require the cooperation of surviving users, a prearranged takeover by EOP/NCS of a user's hub station, or a priori dedication of spacecraft assets. When utilizing a shared transponder, intermodulation distortion caused by amplitude and phase nonlinearities in the transponder can degrade performance. Furthermore, a jammer or a user transmitting at too high an output level can drive the satellite transponder into saturation (nonlinear operation), rendering the transponder useless to other users. During times of stress these remaining assets are tightly controlled by the established procedures mentioned in Section 2.

All the spacecraft available to support a VSAT system operate in a geostationary orbit in the equitorial plane at longitudes between about 75° West and 130° West. In the Ku and Ka-bands, the frequency assignments for CONUS (Region 2) are nominally as shown in Table 3-1. Most of these allocations are for exclusive satellite use; hence, no coordination with terrestrial radio system users is required, as is the case with C-band frequencies.

The bandwidth of a typical (e.g., RCA) Ku-band transponder is 54 MHz, but could still be 36 or 72 MHz. For full-CONUS coverage the effective isotropic radiated power (EIRP) of the RCA Ku-band transponder is nominally 43 dBW and increases to a nominal 47 dBW for half-CONUS coverage. Direct broadcast satellites at Ku-band typically use 36 MHz bandwidth transponders with EIRPs of 49 to 56 dBW. The receiver figure of merit for

these satellites is in the range of -2.5 to +5 dB/K, with the higher ranges being for direct broadcast satellites.

The ACTS, operating at Ka-band, incorporates an electronic scanning multibeam antenna in conjunction with on-board switching and processing. There are three beams active simultaneously, each with 750 MHz bandwidth and an EIRP of 56 dBW, and the receiver figure of merit of 14.2 dB/K. The ACTS also has a mechanically steerable antenna with equivalent EIRP and receiver figure of merit.

3.1.2.3 Earth Station

The typical, inexpensive VSAT Ku-band earth station consists of a 1.8-meter dish antenna, a 2-watt solid state amplifier, and a low noise receive amplifier with an equivalent noise temperature of about 290K. Typical transmit EIRPs (at 14 GHz) are 49.5 dBW and a receiver figure of merit (at 12 GHz) of 19.3 dB/K. Smaller terminals with 1.2-meter antennas and about 3-4 dB lower figures of merit, are also available. These terminals are easily transportable but the antenna pointing accuracy (to the spacecraft) dictates installation on a stable concrete pad.

Ground terminals proposed for the ACTS system use 1.8, 3, and 5-meter antennas, although smaller antennas are possible (e.g. an airborne 0.7-meter antenna is also proposed). The 1.8-meter antenna will achieve an EIRP of approximately 56 dBW with a 2-watt solid state amplifier and a 24 dB/K receiver figure of merit. Again, installation on a stable pad is required in order to maintain the needed antenna pointing accuracy.

Modulation normally employed is binary phase shift keying (BPSK) or quadra phase shift keying (QPSK) with rate 1/2 or rate 3/4 convolutional forward error correction (FEC) coding and sequential decoding. VSATs usually employ frequency division multiple access on each transponder, in which one frequency is assigned to each user group. The user group can then establish its desired protocol for controlling the assets provided by the carrier.

Table 3-1. VSAT Frequency Assignments

USE	UPLINK BAND	DOWNLINK BAND
Direct Broadcast		12.2-12.7 GHz
Uplink Feeder for Direct Broadcast	14.0-14.8 GHz 17.3-17.7 GHz	
Fixed Satellite (VSAT)	14.0-14.8 GHz 27.3-30.0 GHz	11.7-12.2 GHz 17.7-20.2 GHz

These assets correspond to a 56 kbps channel (to/from a hub) and many users served multiple sites using random entry time division multiple access (TDMA). These systems are not normally designed to carry traffic remote-to-remote. However, using standard link budget equations, it can be shown that limited remote-to-remote traffic can be supported. The remote-to-remote supportable data rate depends primarily on how the transponder is utilized. If a remote wishes to transmit to another remote and must compete with numerous high power hub uplinks, the supportable data-rate may be 75 bps or none at all. On the other hand, if the entire transponder were dedicated to supporting remote-to-remote traffic only, data rates of 9.6 to 56 kbps could be supported depending on the number of user groups sharing the transponder.

The ACTS system can support much higher data rates due to the higher antenna gains. Supportable site-to-site data rates are typically 1.5 Mbps for 1.8-meter antennas and 256 kbps for 1-meter antennas. Because of the hopping spot beam used on ACTS, these are TDMA burst rates.

3.1.2.4 Availability Considerations

Both Ka- and Ku-band signals are subject to attenuation and degradation due to precipitation. This effect will be felt the most in high rain regions (SE CONUS) and at earth station locations with low look angles to the spacecraft. The degradation gets worse as the frequencies go up. Typically, 99.5% availability can be achieved with 2 dB of margin at 20 GHz and 10 dB at 30 GHz. In general, rain outages are of short duration (minutes); hence, they are not a major consideration for reconstitution situations.

3.1.2.5 Interface, Employment and Control

A VSAT star method network utilizing a large hub earth terminal is readily adapted to the reconstitution problem. Off-the-shelf systems exist that support a 56 kbps FDMA carrier on a shared transponder using a standard interface. Scientific-Atlanta, Inc. has introduced what they call an Intelligent VSAT that supports four RS-232 ports for local devices at speeds up to 19.2 kbps. The system comes with IBM PC-based software that uses X.25 to support IBM's Systems Network Architecture, SDLC, and bi-synchronous protocols. The X.25 support enables the VSAT to be connected to public switched networks. Network control is performed at the hub, but each VSAT has access to the hub and can perform network reconfigurations. Numerous other vendors have similar products that conform to current standards and/or de facto emerging standards.

The configuration and control of a mesh network consisting of all VSATs requires engineering and development for access and control since such off-the-shelf systems are not currently available (but may be forthcoming). The basic VSAT off-the-shelf terminal could be employed with standard access schemes but a control system must be designed. In

addition, agreements with satellite carriers must be made to ensure that the transponder loading is such that an all VSAT network can be supported.

The use of ACTS requires considerably more planning and engineering. The ACTS satellite is not yet launched and current plans call for performing experiments during the first two years of operation, approximately 1990-1992. Plans could be made now to perform some experiments specifically for DCS data services reconstitution during this time period and have this asset available in the later life of ACTS. Particular issues that must be addressed are point-of-entry, functional and electrical interfaces, protocols, and subnet control.

A separate, but important, control issue surrounds telemetry, tracking, and control (TT&C). The spacecraft owner/operator (i.e., the commercial carrier) employs a control facility to maintain the spacecraft bus, communications system, and orbital position. This same facility also manages major features of the communications payload. The user only controls the assets assigned to him and his own subnetwork. Hence, the user is dependent on the control facility and TT&C managed and maintained by the carrier. No single interest community will be permitted to control this facility in the event of a crisis. Therefore, the DCS data services reconstitution requirements again must be addressed through DCS/NCS channels to the controlling element of the National Command Authority. The best that can be reasonably accomplished is administrative agreements and cooperation exercised through established forums.

3.1.2.6 Security Considerations

The security requirements discussed in Paragraph 2.5 include protection from compromise, protection of data integrity, and protection from denial of service. The satellite channels are nonsecure because of the beamwidth of the satellite antennas. Any transmitter operating within the bandwidth of the satellite transponder and within view of the satellite's receive antenna can jam the channel by transmitting a powerful signal, driving the transponder into saturation. Spread spectrum techniques are used to reduce susceptibility to jamming by up to two orders of magnitude. Convolutional forward error correction (FEC) coding, interleaving, and sequential decoding are used to improve bit error rate performance. Data encryption is used to protect data from compromise.

3.1.3 High Frequency Radio

3.1.3.1 The Characteristics of HF Radio

The HF spectrum is defined as the region from 3 to 30 MHz. HF radios are typically single sideband, amplitude modulated with channel bandwidths of 3 KHz. The HF radio channel is characterized by constant change in propagation characteristics, necessitating periodic changes in frequency during each 24-hour period. The channel is also subject to fading and

is susceptible to man-made and atmospheric noise. However, it does provide the capability for wireless, transcontinental voice and data communications. HF characteristics include:

* The major modes of propagation of HF radio waves are groundwaves and skywaves. Groundwaves are useful for relatively short distances. For beyond-the-horizon paths, skywave propagation is dominant.

* Skywave propagation makes use of the refraction (reflection) of HF radio waves by the ionosphere. These reflections occur at altitudes of greater than 100 miles.

* To be refracted back to earth, skywaves must strike the ionosphere at angles less than or equal to what is called the critical angle. Skywaves striking the ionosphere at angles greater than the critical angle pass through the ionosphere. The critical angle varies inversely with frequency. Multiple hops are also possible, wherein the skywave returning to earth is reflected by the ground.

* There is a minimum distance at which skywaves return to earth, called the skip distance. The skip distance increases with increasing frequency.

* Electron density variations change the reflectivity of the ionosphere and its absorption.

* Changes in electron density result from ultraviolet radiation and other forms of energy from the sun impinging on the atmosphere. These changes occur on a diurnal basis and vary with the seasons, being strongest in summer. Solar flares, which occur periodically, cause sudden, drastic changes in the ionosphere that impact HF radio propagation severely for a period of hours or days. Sunspot activity, which varies over a 9- to 13-year cycle, also affects HF radio propagation.

* Because of diurnal electron density variations, the same transmit frequency cannot be used throughout a day. At night, when electron density is low, lower frequencies must be used than are possible during the day.

3.1.3.2 The Performance of HF Radio in a Reconstitution Environment

The majority of existing HF radio systems are not reliable for data transmission because of the constant changes in the composition of the ionosphere and the age of the equipment. In addition, the ionospheric disturbances expected to result from high-altitude nuclear detonations may make HF radio communications impossible for hours or days. A typical application of HF radio is to patch telephone calls once an HF circuit is established. These hookups can also be used for data transmission at data rates up to 2.4 kbps, including the transmission of packetized data. At the present time, HF radios do not have a packet switching capability, but research in that direction is taking place. HF radios are widely used

by federal agencies and the Department of Defense (DoD), so their use for reconstituting communications emote users should not be overlooked.

3.1.3.3 Security Considerations

The security requirements discussed in Paragraph 2.5 include protection from compromise, protection of data integrity, and protection from denial of service. By its very nature, the HF radio channel is insecure in that signals can be detected over a very large area. Thus, to provide protection from compromise, data encryption will be required. The HF channel is also very susceptible to jamming from sources distant from the receiver. Some forms of spread spectrum, such as frequency hopping, can be used to mitigate the jamming threat. Frequency hopping can also be used as a multiple access scheme through the use of orthogonal hop addresses among network users.

3.1.3.4 Other Considerations

Federal agencies and the Department of Defense are currently working on standards for a family of automated HF radios that will have the following capabilities. These enhanced HF radios should make HF radio a useful element for DCS data services reconstitution. Other considerations include:

* Automatic link establishment whereby the user keys the address of destination and the radio automatically handshakes with the destination radio to select the optimal frequency to use before establishing the link

* Message store and forward

* Data transmission at 2.4 kbps

* Packet radio at 2.4 kbps

* Digitized voice at 2.4 kbps

* Frequency hopping for antijamming and interference reduction.

3.1.4 Meteor Burst

3.1.4.1 The Characteristics of Meteor Burst Communications

Meteor burst communication makes use of the ionized trails produced by meteors entering the Earth's atmosphere to reflect radio waves to a receiver beyond the horizon. These ionized trails are short lasting (around 0.5 sec) but are plentiful enough (several per minute) to support a modest but reliable throughput of information with appropriate system design.

With the advent of inexpensive microprocessors, meteor burst technology has become of age; it is reliable and available off-the-shelf.

Many of the characteristics of meteor burst communication are dictated by the laws of physics and the orbits that meteors follow around the sun before they encounter the Earth. The design of the meteor burst communication system and the siting of the terminal equipment also influence the throughput (bps) and waiting times for message or packet delivery (secs). The following characteristics of meteor burst communications are dictated by the physics of reflection from columns of ionization:

* Throughput is a function of frequency over the useful frequency range (15 MHz to 120 MHz) being greatest at the lowest frequencies other factors being held constant. Having chosen a frequency, there is no need to change it (as is the case with HF radio).

* Throughput is a function of transmitter to receiver range being greatest at about 1100 km (680 miles) (Reference 4). With reduced performance, meteor burst communication will work at all short ranges until line of sight or ground wave propagation dominates. At longer ranges horizon effects reduce performance gradually to a cut-off point around 1800 km (1100 miles).

* Throughput is maximized if antenna design is matched to the size and location of the hot spots of meteor activity on the given circuit. Broader and narrower antennas than the optimum result in reduced throughput.

The following characteristics of meteor burst communication are dictated by the orbits of meteors around the sun:

* Throughput varies with time of day and time of year. Performance is best at 06:00 and worst at 18:00 over a wide range of low to mid-latitudes. In the Northern hemisphere, performance is best in June and worst in early February.(Reference 53)

* Throughput varies with latitude falling off considerably above 60° latitude (Reference 4).

The following degrees of freedom may be used in the design of meteor burst systems to maximize performance on a given link (or network).

* Man-made noise is a severe constraint on meteor burst system performance. Quiet receiver sites, and modems designed to handle bursty noise can greatly improve performance.

* Throughput increases with transmitter power and instantaneous transmission rate.

* Systems are available that use a variable transmission rate - high at the beginning of the burst when S/N is high, and reducing toward the tail of the burst. This technique can double the throughput on a given system (Reference 37).

* The use of diversity can improve throughput. Antenna height diversity is the most useful diversity technique because it increases the coverage of the useful volume of the ionosphere. Cross-path antenna diversity and frequency diversity are less useful increasing throughput only through uncorrelated fading in the tails of long bursts (Reference 1).

* Optimizing antenna patterns to the link can greatly improve performance. Antenna height above the ground, and tilt and offset angles with respect to horizontal and the great circle path, respectively, are important parameters. As stated above, antenna beamwidth should be optimized to the link.

* Adaptive antennas are a promising technology for meteor burst communications (Reference 4). This technology is not yet available for meteor burst applications.

Regulations concerning the use of the radio frequency spectrum restrict the frequency range that can be used for meteor burst communications. In North America, certain parts of the 40-50 MHz band may be used. In Europe, lower, and hence better, frequencies are available. It may be possible in a reconstitution situation to obtain authorization to use frequencies that would otherwise be unavailable. For example, some part of the band 30-40 MHz used normally for TV broadcast in North America, could possibly be made available for reconstitution following an attack causing widespread damage. Until such issues can be resolved in the appropriate forum, it is wise to assume that existing frequency regulations will apply post-attack.

3.1.4.2 The Performance of Meteor Burst in a Reconstitution Environment

Existing meteor burst technology operating in the 40-50 MHz band can be expected to provide a worst case throughput of 100-200 bps on a well designed 1000 km point-to-point link using directional antennas. If this link were used to provide a user access to a DISNET node, that user could expect quite large delays to packets (on the order of minutes) and therefore rather poor performance in an interactive application. Up to four times more throughput could be expected at better times of the day and year. Very short links, just beyond line-of-sight and groundwave propagation distances, could expect 1/3 to 1/2 of the 1000 km throughput. Links designed with non-directional antennas would be considerably worse except on the short links where 30-100 bps would still be possible.

Meteor burst communications in the 40-50 MHz range recover quickly from any effects from high altitude nuclear explosions and would be available in a post-attack environment, provided only that the terminal equipment survived. By the use of quick-erect towers, meteor burst could provide a rapid restoration capability.

Meteor burst links with their *store and burst* transmission environment, place different demands on crypto equipment than do full period links, but crypto equipment can be used with meteor burst links both for communications and traffic flow security. It is also interesting to note that the meteor burst medium provides a degree of inherent privacy (Reference 31). The burst that provides communications to the intended receive site cannot be heard, except by rare occurrences of two simultaneous suitably oriented meteors, more than about 50 km from that receive site. At the lower frequencies, particularly those below 40 MHz, propagation modes such as sporadic-E can yield, at certain times of the day and year, relatively high throughput on a meteor burst link at the expense of this inherent privacy.

3.1.4.3 Security Considerations

The security requirements discussed in Paragraph 2.5 include protection from compromise, protection of data integrity, and protection from denial of service. The meteor burst channel is relatively secure in that a signal being received at a particular site can rarely be intercepted by a receiver more that 50 kilometers away. This also means that jamming of the signal is difficult except by jammers near the receive site. Data encryption and coding techniques can be used to protect data from disclosure and to maintain data integrity, respectively.

3.1.5 Switched Telephone

Switched telephone, commonly referred to as dial up, refers to establishing a connection on a 2-wire voice grade switched circuit using a standard telephone instrument, and employing a modem for the data connection. The circuit can be provided by DSN or a public switched network. Once the connection is established, the circuit is used as a regular dedicated data circuit. The majority of voice grade circuits currently use analog interconnect media or consist of a mixture of analog/digital media, therefore limiting the use of voice grade connectivity to lower data speeds. This limitation is due to less stringent circuit quality parameters found on voice grade circuits and imposes data rate limits of no more than 4.8 kbps with current technology. Use of the STU-III for voice/data communications is one version of this type of switched telephone connectivity and is discussed below.

Figure 3-3 illustrates the configuration by which several voice/data end-users are connected within the DCS/DSN/DDN system. A voice/data end-user at Site A is connected through the shared local fixed-plant cable distribution system to a remote packet switch node at Site B. This interconnect is accomplished through shared off-post commercial or Government-owned DCS transmission facilities. Primary connectivity is provided via hardwired service between the data end-user and its supporting packet switch. Alternate connectivity can be provided to either the same PSN or a designated alternate PSN via the common-user telephone line associated with a collocated telephone instrument, found at the same end-user location. This connection can be established using a variable or fixed rate data dial up modem, at a transmission speed suitable to the voice grade interconnect facilities. Site B

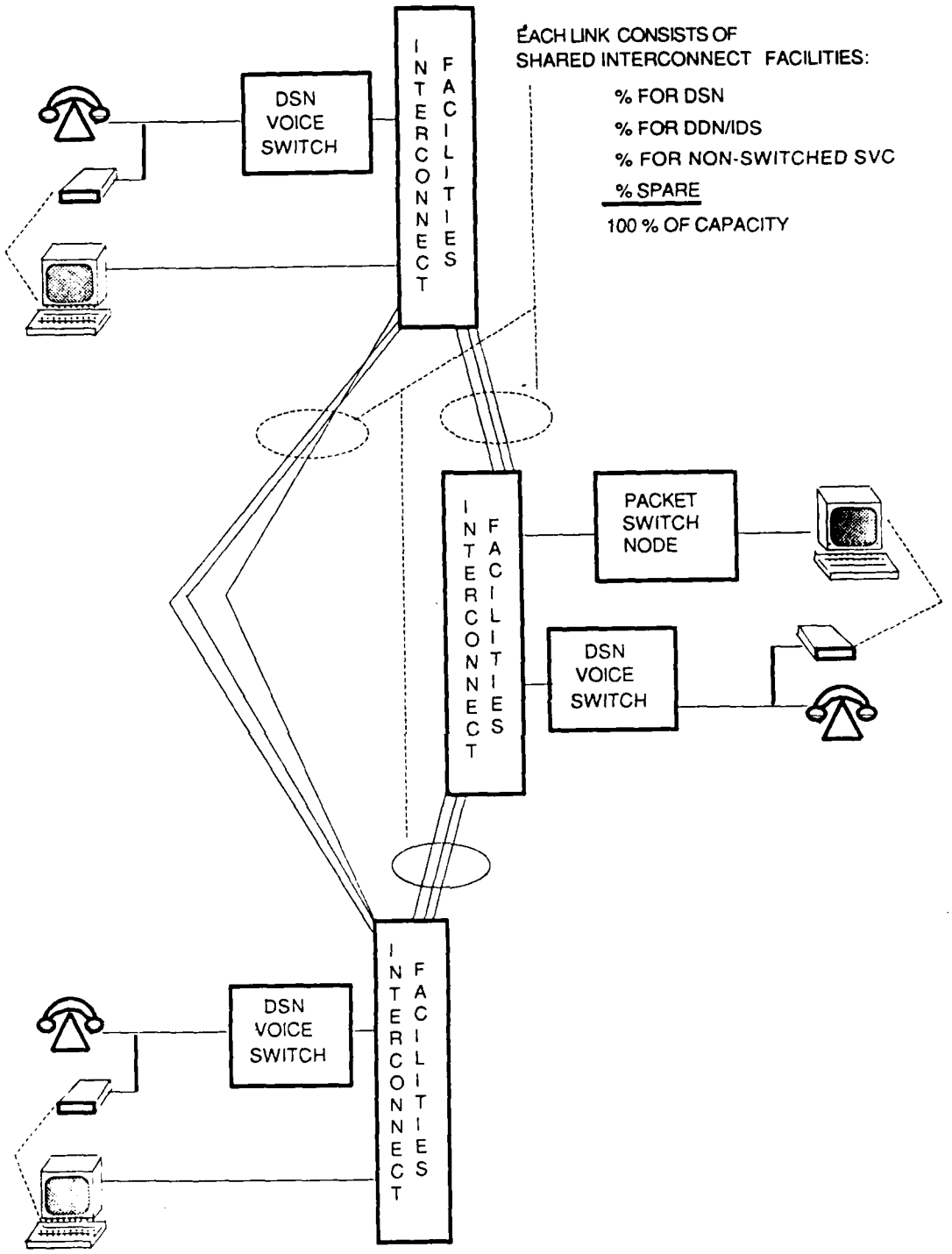


Figure 3-3. Dial Up Access Configurations

data users are connected to their collocated Packet Switch through a shared local fixed-plant telephone cable distribution system. Dial-up modems are of little value if the DSN voice switch and packet switch node facilities are collocated at the same site with the supported data end-users. It can be assumed that if the local packet switch is not available to the end-user, the voice switch is also not likely to be available. Notice that none of these end-users or switches connect directly to each other; electrically they are interconnected, but physically they are connected via shared local cable distribution plant through the off-post shared commercial or Government-owned DCS transmission facilities.

Use of voice grade lines rather than the designed data grade circuits will effectively limit data throughput rates to slower data speeds. Additionally, it must be remembered that use of dial-up connectivity would provide limited access to telephone lines that will be seriously competed for by all voice and data end-users at that site, where the common user voice traffic generally has the lowest circuit restoration priorities. Dial-up access provides apparent flexibility to the end-user, but actually has very limited practical application and employment can be very scenario dependent. If the local packet switch is not operational due to any hostile action, the adjacent voice switch can also be expected to be affected by collateral damage; if a remote packet switch is not accessible via dedicated connectivity, then an end-user may be able to reconnect through a dial-up modem to another packet switch; if there are switched voice circuits available, then a modem at the end-user and the new data switch would allow some communication if any connection could be made.

User locations having access to a STU-III secure telephone terminal device that operates over standard 2 or 4 wire telephone access lines and provides a secure data capability may be able to use this device for secure restoral of limited low speed data (i.e., point-to-point data service). In the data mode it can operate at speeds from 300 to 4800 baud synchronous/asynchronous (varies based on the manufacturer as shown in Table 3-2) and is equipped with an RS-449/RS-232 compatible interface. Since it is envisaged that most high priority users will be provided STU-III equipment for voice service, those that require reconstitution of their DCS data services should have immediate access to a STU-III terminal. It must be remembered that successful use of STU-IIIs or any other terminal equipment with dial-up connectivity requires similar equipment at both ends of the reconstituted circuit.

3.1.5.1 STU-III Terminals

All STU-III terminal equipments are interoperable and have both a voice and data transmission capability. The terminals that are being provided fall into four basic categories: Telephone\Desk Top, Cellular Radio, Tactical, and Personal Computer. A brief description of each follows.

* Telephone/Desk Top - This is the primary terminal that is being manufactured and is referred to as the Low Cost Terminal (LCT). Since it is being manufactured in large quantities and by three companies, it will be the most affordable. There are

two variations of the LCT. LCT-1 is designed to provided encryption of DoD classified information and LCT-2 is designed for privacy protection. The terminal interfaces include the standard telephone 2-wire, 4-wire and multiline (1A2 key system) compatibility. The data terminal equipment interface is RS-449/232 compatible. The data line speeds vary according to the manufacture. See Table 3-2 for additional details.

* Cellular Radio - The cellular radio version is being manufactured by Motorola. It has an RS-232C interface for use with an external data terminal and can accommodate 2400 bps synchronous; and 300, 1200, and 2400 bps asynchronous. The terminal is designed for vehicular installation.

* Tactical - The tactical terminal, referred to as the Mobile/Portable Terminal (MPT), is also being manufactured by Motorola. The STU-III/MPT is a ruggedized, mobile/portable unit consisting of a tactical handset. The tactical handset provides a standard keypad for dialing, buttons for on-hook/off-hook control, push-to-talk switch, and a microphone/earphone elements. The MPT is intended to satisfy the requirements for STU-III compatible secure communications in field, mobile/portable, and airborne environments. It will extend STU-III operating modes to users requiring applications with radio nets, external modems, and dedicated ("hot line") circuits.

  This terminal has a wide range of interfaces. In addition to the standard telephone wireline interfaces, it has the capability to interface military type radios (MIL-STD-188C levels), cellular radios (Motorola proprietary), and an external modem with a black digital signal at 2400 bps. The data terminal equipment interface is

Table 3-2. STU-III Vendor Data Modes (LCT-1)

MODE	SYNCHRONOUS				ASYNCHRONOUS			
(Bits per Second)	300	1200	2400	4800	300	1200	2400	4800
Clear Data			AT&T	AT&T			AT&T	AT&T
Secure Data			AT&T*	AT&T		AT&T	AT&T	AT&T
		RCA	RCA*			RCA	RCA	
			Motorola*		Motorola			
						Motorola		
							Motorola	

*Basic Feature

RS-232C compatible, full and half duplex, and will accommodate 2400 bps synchronous; and 300, 1200, and 2400 bps asynchronous. The MPT will also operate in a dedicated "Hot Line" mode which is unique to this terminal and may have application in some reconstitution plans. The connectivity between the MPTs can be either a dial-up circuit (nailed- up) or a private line. The terminal is capable of signaling the far end terminal when the near end goes off hook. The terminal can be controlled to go on or off hook as the service requirements may dictate. Motorola has advised that this terminal could be modified to operate up to 64 kbps.

* Personal Computer (PC) - A portable PC terminal that is totally IBM-PC compatible will be available from Motorola . Called GRiDSEC, it is a combination of GRiD Systems portable TEMPEST computer and Motorola communications equipment. The terminal provides rugged portable secure voice or data communications to other STU-III terminals at 2400 baud. Its integrated packaging allows sending data securely with no added accessories along with providing extensive computer capabilities. The terminal will interface with standard telephone systems, cellular radio, and a variety of uhf/vhf radios.

3.1.5.2 STU-III Equipment/Key Management

A major ingredient in any reconstitution concept is the encryption of digital links connecting reconstitution assets to either the network or to the user facilities. Encryption requires Key Generator (KG) equipment and keying material.

The distribution and control of the keying material for most data encryption devices constrains where and when an IST or access circuit can be rehomed. Keying material, which is classified at the highest level of traffic that is to be protected, must be positioned at each location where a circuit will be rehomed and in sufficient quantity so once the circuit is activated the KG can be rekeyed on a regular basis (i.e., every 24 hours) until new keying material can be furnished through normal distribution. Resupply can take several days and sometimes weeks. The long acquisition lead time makes it very difficult to react to emergencies that dictate changes in the network configuration or user requirements. Consequently, plans for reconstitution must consider all possible contingency rehomes to ensure that each circuit (KG pair) can be properly equipped with keying material.

The STU-III equipment implements the FIREFLY II keying algorithm and functions. The initial keying material is inserted into the terminal by means of a fill device (FD). After loading, the FD is converted by the terminal to a crypto-ignition Key (CIK). This conversion is done in a self-protective manner, so that when the CIK is separated from the terminal neither the terminal nor the CIK is classified. Each CIK is bound to the terminal that created it and is thus unique to the terminal. In addition, built-in protection mechanisms allow for key changes only once each year.

After a terminal is loaded with its initial key, secure calls/connections can be made to any other STU-III terminal. When the terminals are connected in the secure mode the terminals generate per- call working keys and crypto-synchronization is automatically accomplished between the two terminals in approximately 12 seconds. Since the terminals generate the key, separate keying material is not required nor is the terminal constrained to any specific KG pair.

3.1.5.3 Security Considerations

The security requirements discussed in Paragraph 2.5 include protection from compromise, protection for data integrity, and protection from denial of service. Switched telephones, in general, are deficient in all three areas. STU-III is an exception; it provides User-User authentication as well as protection from compromise, but is still deficient in providing protection for data integrity and protection from denial of service.

3.2 Technology Employment for Reconstitution

3.2.1 Advantages/Disadvantages of Packet Radio

Packet radio systems, such as the DARPA Low Cost Packet Radio will provide a high quality reconstitution medium for subscriber areas. Through proper planning and deployment of repeaters, it can also provide an excellent access area and short range backbone reconstitution medium. Its main disadvantage is its limited range, which requires the use of repeater stations to maintain line-of-sight paths. VHF radio systems can provide greater coverage but at data rates of at most 16 kbps.

3.2.2 Advantages/Disadvantages of Very Small Aperture Terminal

The use of VSATs for reconstitution is extremely attractive because of the low cost and availability of terminals and the fact that numerous satellites supporting VSAT networks are and will be available in the 1990s. VSATs especially incorporate standard interfaces and protocols and can, therefore, be readily interfaced with other systems. VSAT networks can be established with as few as only two terminals and support is possible for up to hundreds of terminals. As is true of all satellite systems, VSAT networks are distance independent. That is, a coast-to-coast link is as easy to establish as a 50 mile link. VSATs can be used to interconnect fragmented terrestrial subnetworks. It is possible to configure VSAT networks with protocols and control compatibilities with most other systems. This will require pre-planning and perhaps the acquisition of non-off-the-shelf equipment. The proliferation of VSATs throughout CONUS suggests that in a post-attack environment assets will be available to establish networks with terrestrial tail circuits posing the only problem. Lastly, supportable data rates of 56 kbps are common for VSATs and using ACTS, T-1 rates are possible.

There are four main disadvantages to use of VSATs for reconstitution. Because of available spacecraft assets, VSATs can only provide service in CONUS. VSATs require accurate pointing and must be pad mounted; hence, they cannot support mobile users. Outages of minutes (or even tens of minutes) can occur due to heavy rain, since VSATs operate in the Ku- and Ka- frequency bands. Spacecraft are controlled at non-survivable control facilities. In a post-attack environment such a facility could be lost with the possible resultant loss of the spacecraft. The time from the loss of the control center to loss of the satellite could be days or perhaps months. Loss of attitude control is the most probable cause of loss of satellite capability.

3.2.3 Advantages/Disadvantages of High Frequency Radio

The principal advantages of HF radio are that it provides a medium for long range communications, both point-to-point and broadcast, and its widespread use within the Federal and DoD communities. It is especially useful for communications to and among mobile users. The disadvantages are the constant variability of the propagation medium, frequency congestion from its widespread use, and the low data rate (2.4 kbps maximum) limit.

3.2.4 Advantages/Disadvantages of Meteor Burst

Meteor burst communication due to its robust nature has advantages post-attack for reconstitution of connectivity. Its low data rate capability (of a few hundred bps) is more suited to a reconstitution order wire than to a DDN access link. Meteor burst would be a good medium to use to determine what other DDN assets survive and where connection is possible - a sort of reconstitution tool rather than the reconstitution medium itself. Perhaps for certain DCS data services applications where a small number of bits are involved and fast response times are not critical, meteor burst could also function as the DDN access link itself.

3.2.5 Advantages/Disadvantages of Switched Telephone

The advantages of the STU-III are its built-in security and data capability, its direct access to DSN, and its availability to the user. A disadvantage is the limited data rates available.

3.3 Interface Modems for Reconstitution

The requirements for interface devices will be accentuated in a stressed environment. Regardless of the interconnect carrier media, some form of compatible interface device will have to be employed to make use of whatever raw transmission facilities exist in a post attack or post war environment. The basic interface device found in the data world for wide-area connectivity has traditionally been modems running at rates under 9.6 kbps. The future of the modem industry has predicted a migration toward higher speed, synchronous,

and more complex modems. While these emerging trends may become a reality for the day-to-day operating world, there will continue to be a place for the slower speed, less sophisticated modems. This is particularly true during times of stress, when the quality and quantity of the surviving interconnect facilities will be questionable and limited. The data user must be prepared to use lower speed, potentially noisy voice grade circuits over limited capacity links using switched or point-to-point connectivity. It is entirely possible that the inventory of interface devices will include both high and low speed modems; the high speed modems for everyday use and the lower speed modems as part of a reconstitution package for interfacing during restricted operations expected in the stressed environment.

The focus of this discussion will be on the low speed modems, since the focus of this report is reconstitution planning strategies. The two most common types of modems in the under 9.6 kbps category are the asynchronous 300, 1200, and 2400 bps modems and the 4.8 kbps synchronous modems. Standards for the asynchronous group include CCITT V.22bis, V.22, and V.26 and Bell 212A and 103. Full duplex mode of operation is the most popular configuration. The 4.8 kbps synchronous modem group are used almost exclusively in the half-duplex mode. Several standards exist for the 4.8 kbps modems: V.32, Bell 208, etc.

It should be noted that asynchronous modems often accept synchronous input, and many synchronous modems can be configured for asynchronous operation. If the correct type modems are not available, asynchronous-to-synchronous or synchronous-to-asynchronous converters will be required.

There are a wide variety of modems found in the commercial market place. When selecting modems for use as part of a reconstitution asset package, care most be taken to adopt only the most flexible and adaptable modems available. Price tag is not the only consideration; in a worldwide network, interoperability and flexibility will be the keys to successful operations in a stressed environment. Several manufacturers are trying to satisfy the demand by producing bare-bones modems and offering field-installable hardware modules that add enhanced features. This modular approach may be especially useful during periods of uncertain connectivities. One area that is being discussed extensively by the industry is the development of an internationally accepted error-correction standard.

The question that has yet to be resolved is "Which error-control protocol will become the internationally endorsed CCITT standard?" The two contenders are the Microcom Networking Protocol (MNP) or Link Access Procedures M (LAP M) (a derivative of the Hayes LAP B standard). CCITT is currently developing specifications for its new V.42 modem error-control protocol. Recently, the CCITT committee developing the standard unanimously agreed that both LAP M and MNP would be included. Under this compromise arrangement, two communicating modems that both support V.42 will use LAP M. However, if an MNP modem interconnects with a V.42 modem, the V.42 modem will use MNP. If the committee were to abandon its compromise support of MNP, a two

standard marketplace would result, inflicting a hardware incompatibility into the operating environment.

Other error-control technique, such as adaptive packet assembly and adaptive equalization, haven't been subjected to such competition. DDN planners should look for both features when considering which modems to use. Adaptive packet assembly is included in MNP Class 4; most dial-up modems include adaptive equalization. Both increase a modem's tolerance for line faults, and both work in conjunction with other error-control protocols.

Modems using adaptive packet assembly send smaller data packets as lines get nosier to minimize the time required for retransmissions. Adaptive equalization is used by modems to de-emphasize received signals containing distortion or noise, thus making the received signal more intelligible.

Some of the many factors that must be considered when determining the interoperability and flexibility of modems to be used in the DDN are: standards, compatibility, error correction, software, security, transmission speeds, and modularity. Some of the available features, either built-in or modular, include: nonvolatile memory, automatic logon, local and remote diagnostics, adaptive equalization, data compression, synchronous input capability, multiple speed conversion, and support of remote network management. The modems chosen to support any form of day-to-day operations and reconstitution efforts should be compatible with as many of these factors and features as possible. This will ensure maximum flexibility and adaptability from a hardware interface perspective. In addition to these considerations, care must be taken to avoid proprietary software situations where the Network could become single vendor sensitive and where a disjointed fragmented Network would have interoperability problems reconstituting the post-attack or post-war Network.

SECTION 4 - Potential Reconstitution Interconnect Resources

As stated earlier, the interconnect component of the DCS data network depends on resources shared with the total communications community and provided by the DCS. The competition for these finite resources requires all user subnetworks to clearly articulate their individual needs within the framework of established practices and procedures. Successful day-to-day operation of the DCS depends on the orderly employment of these rules. Times of stress generally dictate an even closer adherence to established reconstitution plans and service restoration rules in order to prevent total chaos. The reconstitution plans of each subnetwork and those of the overall DCS/NCS must be closely integrated in order to provide any reasonable level of communications support to the surviving community of customers. The type of media available to support DCS data network needs can be viewed from two perspectives: technically and operationally. The tables included herein provide a summary overview of the potential types of interconnect service that exist in the inventory.

4.1 Technological Considerations

Table 4-1 contains a technological comparison and summary of the interconnect concepts discussed in Section Three and, also, contains some types of media that have not been fully addressed in Section 3. Technically all these media have established interfaces between the different modes, so if more than a single type survives, and is available, they can be linked to provide long distance end-to-end service. It is quite common in the pre-stress environment to have service provided over several links tying two or more user locations together and for these links to be made up of multiple types of interconnect facilities. At this time it is necessary to provide some focus on the individual headings contained in the table. Following is a list of the headings and an explanation of their contents:

1. Distance: A statement of the average operating distance for a single repeaterless link using a particular type of media.

2. Data Rates: An expression of the typical throughput data rates for a given media.

3. Frequency Range: The normal operating range for the specified media.

4. Mode: Analog or Digital

5. Interface Requirements: Identifies the physical hardware/software required to interface the terminal/packet switch component of DCS data network with the selected media. The type of modem, access units, and/or wireline connections.

6. **Reliability:** Quantifies the expected quality of the selected media service based on known performance parameters.

7. **Limitations/Remarks:** Statement of technical factors that must be considered which have not been covered by any other heading, but would need to be evaluated during the media selection process.

Table 4-1. Technical Description/Parameters

Design Considerations / Type of Technology	Technical Parameters: Distance (Miles)	Data Rates (kbps)	Frequency Ranges	Mode A/D	Interface Requirement	Reliability	Limitations/ Remarks
Radio							
HF						Poor	
Ground Wave	<100	2.4	3-15 MHZ	A/D	Modem Rqd		
Sky Wave	500-3000	2.4	10-30 MHZ	A/D	Modem Rqd		Blackout after Nuclear
Meteor Burst	<1100	<.2	40-50 MHZ	D		Good	
Packet Radio	<40	100-400		D		Good	
LOS Radio/Micro	<40	64*	2-20 GHz	A/D	Modem Rqd	Good	
Tropo Scatter	400-700	64*	100-10000 MHz	A/D	Modem Rqd	Poor	
DSCS	<6000	64*	7.5-8.5 GHz	A/D	Modem Rqd	Poor	Satellite/ET Required
VSAT	<3000*		10-30 GHz	A/D	Modem Rqd	Poor	Satellite Required
Cable	N/A		N/A				
Wire						Good	
Analog		9.6		A	Modem Rqd		
Digital		64*		D			
Fiber Optic		64*		D		Excellant	
Dial Up/STU-III		<4.8		A		Fair	

*Per voice channel, data rates are generally provided in multiples of 64 kbps
* Due to spacecraft antenna coverage limitations

4.2 Operational Considerations

Table 4-2 contains some of the operational considerations and a summary evaluation of the employment applications versus the stated levels of stress. Since we are dealing with the shared component of the DCS data network, the interconnect media, the comparative levels of stress used in this table parallel those found in the national/international arena rather than the ones stated in the DDN Program Plan. Following is a list of the headings and an explanation of their contents:

1. Levels of Stress: As contained in the National Security Emergency Preparedness (NSEP) Telecommunications Service Priority (TSP) System (See Table C-3).

2. Recommended IDS Areas: Lists the three areas and identifies the preferred media given the assumed characteristics identified in Section 2.

Table 4-2. Application/Operations Considerations

Type of Technology	Application Considerations: *Applicable Levels of Stress		Recommended IDS Areas		
	2	3	Sub	Access	BB
Radio					
HF					
Ground Wave		X	X	X	
Sky Wave		X		X	
Meteor Burst		X		X	
Packet Radio		X	X	X	
LOS Radio	X	X	X	X	X
LOS Microwave	X	X	X	X	X
Tropo Scatter	X	X	X	X	X
DSCS	X	X		X	X
VSAT		X		X	X
Cable					
Metallic Wire	X	X	X	X	X
Fiber Optic	X	X	X	X	X
Dial Up/STU-III		X	X	X	

*All of these technologies are used in day-to-day operations (i.e., Stress Level 1)

4.3 Summary Comments

It is envisioned that DCS data network reconstitution planning will desire to take advantage of all appropriate media available. Terminal/switch nodes must be flexible and capable of interfacing with a wide variety of media. During periods of reconstitution and restoration, determination of which media to use may boil down to what is available. Therefore, the selection process generally is not an either/or situation. The selection of which interconnect media to use will depend on the specific circumstances of a wide variety of potential scenarios and some of the variables contained in these tables. As mentioned earlier, it is possible to use a mixed blend of media in multiple link applications. In order for the DCS data network system to take maximum advantage of the various interconnect media, particular attention must be made to two important areas: the acquisition of the physical interface between the terminal/switch components and the available media and the rules for establishment of appropriate restoration service priority levels for a identified set of user categories.

SECTION 5 - Employment Considerations for IDS Reconstitution

The development of deployment/employment planning strategies for DCS data network reconstitution is built on a range of adaptive flexible plans and scenarios using the interconnect alternatives identified in Section 3 and summarized in Section 4. These technologies are not restricted to equipment capabilities, but include a blend of pre-positioned plans and the establishment of procedures to be employed during times of stress. The range of considerations for reconstitution planning includes, but is not limited to, hardware/equipment identification; determination of the quantities required; environmental studies to determine the pre-war storage and deployment requirements; employment concepts for use of reconstitution assets within a stressed environment; integration of these assets in the MILDEP inventory; personnel and training requirements; and employment of these assets during JCS simulated exercises on scheduled periodic basis. No attempt should be made to plan for reconstitution of the entire pre-war full service data network, any concept should only address the reconstitution of the range of services provided by the data system and not the total data network itself. Any reconstituted data network must be adaptive and flexibility tailored to support the surviving user population.

5.1 Concept Definitions

Prior to the development of a reconstitution employment concept, it is appropriate to first come to a community-wide understanding of terms. The pre-war data network is a subelement of the DCS and therefore an integral part of the strategic communications system. This is a common-user switched system primarily serving end-users in a non-tactical environment. Equipment used in this environment usually consists of high capacity, large scale, fixed installation components consisting of switch terminals and interconnect facilities. From a communications perspective, the military departments have limited assets available that have been designed to provide for replacement of both link and terminal facilities. Employment of these contingency assets is governed by JCS and controlled through extensive closely coordinated contingency plans. The majority of these assets are classified as "transportable" (i.e., they are designed to be moved into position before being placed in an operating mode). Some of this equipment is pre-positioned in the operating theaters and some is CONUS-based for worldwide deployment. Currently, transportable packet switch terminal assets for use in the emerging data network are not included in the MILDEP inventory. A brief list of terms and associated definitions is included in Appendix A.

5.2 Understanding the Environment

At this time, it is appropriate for discussion purposes to create the framework for development of the necessary reconstitution concepts and planning documents. All available studies indicate that the environment will consist of disconnected enclaves of surviving resources. Therefore, correct application of the appropriate limited interconnect assets will govern the ability of the user community to reconstitute some form of functional capability. Following is a brief presentation of the potential communications interconnect conditions found in three identifiable levels of the environment. The discussion includes the application of short range line-of-sight radios for subscriber/access area interconnect. Adaptations of these scenarios can be made to employ other types or a mixture of media described in Section 4.

5.2.1 Pre-Crisis Environment

The environmental relationships for the networks and subsystems of the DCS discussed in Section 2 are, in effect, in a pre-crisis environment and the projected assets of the mid-1990s DCS, including the future IDS data network once in place. The component subnetworks of the DCS data network primarily consist of MILNET and an integrated DISNET (consolidated DSNET1, 2, and 3) with DISNET providing the required internodal switching capabilities for the residual AUTODIN system. Due to the intended community of interest and the nature of the subscriber, it is assumed that MILNET would hold the lowest priority for reconstitution, while DSNET2 (WINCS) would hold the highest priority. Therefore, the initial focus of reconstitution efforts will be placed on reconstruction of the identifiable component networks of the future IDS which encompasses the highest priority end-users. A key element of all these component networks is identified as the packet switch itself. In the mid-1990s, this switch is assumed to be either a BBN C30 or C300 packet switch. It is further assumed that these operating packet switches are essentially identical in capabilities among the various DDN component subnetworks. There are, essentially, two ways to ensure that these critical switch assets survive and transition over the spectrum of conflict to the post-war environment. The first is to place the switch in the hardened command center with the population it is designed to serve, and the second is to build a transportable switch to be prepositioned in the theater at a location most likely to experience minimal damage. This van-mounted transportable packet switch node must be configured to support DISNET subscribers and must include a suite of communications interface equipment to enable the packet switch node to interconnect with all possible available types of switched or transmission backbone assets. The actual number of required transportable switches and the recommended locations for storage are beyond the scope of this document; this will depend on the undefined evolving architecture of the data network topology. It should be pointed out that extensive studies have been done for the deployment and employment of other transportable command and control (C^2) assets, any

planned use of transportable packet switch nodes must interact with and build on the results of these efforts. For connectivity purposes, low speed line-of-sight radios could be placed with the transportable packet switch node or at the switch located within the hardened C^2 facility to provide an initial interconnect capability on either a host-to-switch or limited switch-to-switch basis. In addition to the radio associated with the transportable packet switch node, a quantity of compatible suitcase radios will also need to be developed. These would be stored with either the transportable packet switch node or possibly collocated with critical survivable host elements. This is generically depicted in Figure 5-1. In this environment, day-to-day operations are being conducted by all elements of the DCS hierarchy and the reconstitution assets discussed above are stored in their designated locations in accordance with established contingency plans.

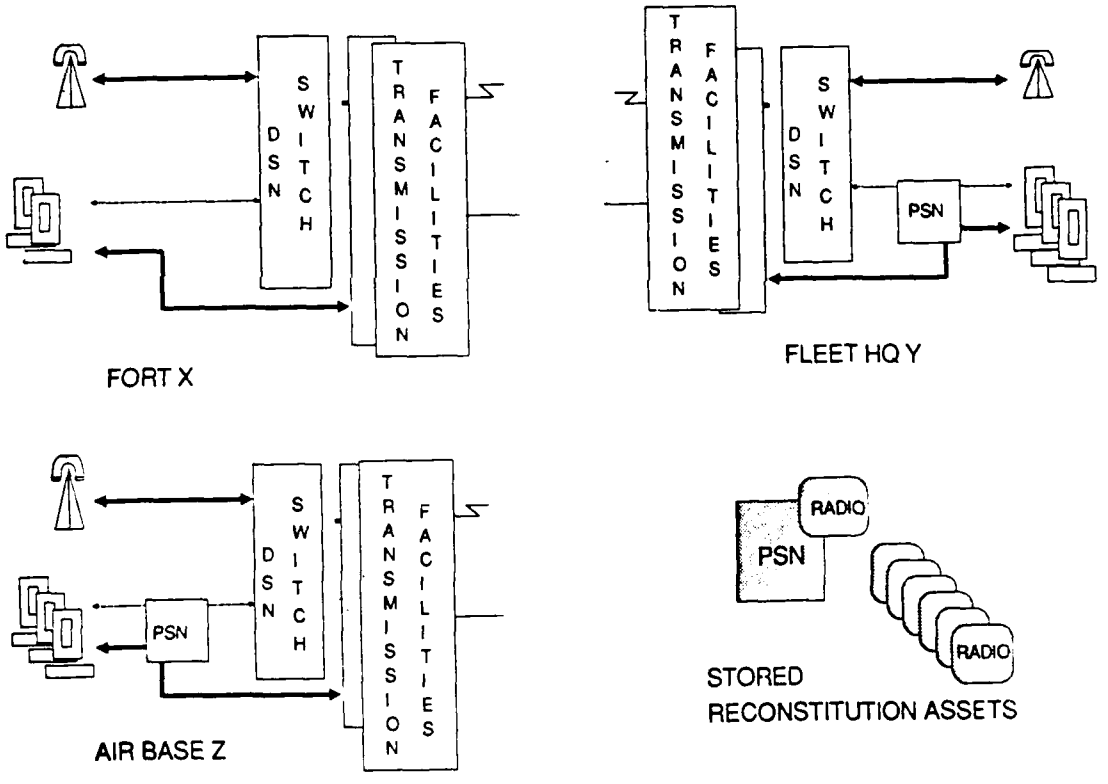


Figure 5-1. Pre-Crisis Environment

5.2.2 Stressed Environment

Figure 5-2 illustrates a potential scenario in which several key elements have been destroyed or disabled: Fort X has lost its switching and transmission facilities along with some of the remote subscribers; Fleet Hq Y has lost its packet switch node and some subscriber terminals; and Air Base Z essentially remains intact. Both terminal hardware and interconnect facilities have been damaged or destroyed at multiple locations. Thus, the stage is set to begin the reconstitution process. Since much chaos and confusion is expected during and shortly after the initial hostilities, critical plans and procedures must be developed and exercised in advance of the crisis and are crucial to any hope for reconstituting the fragmented data networks.

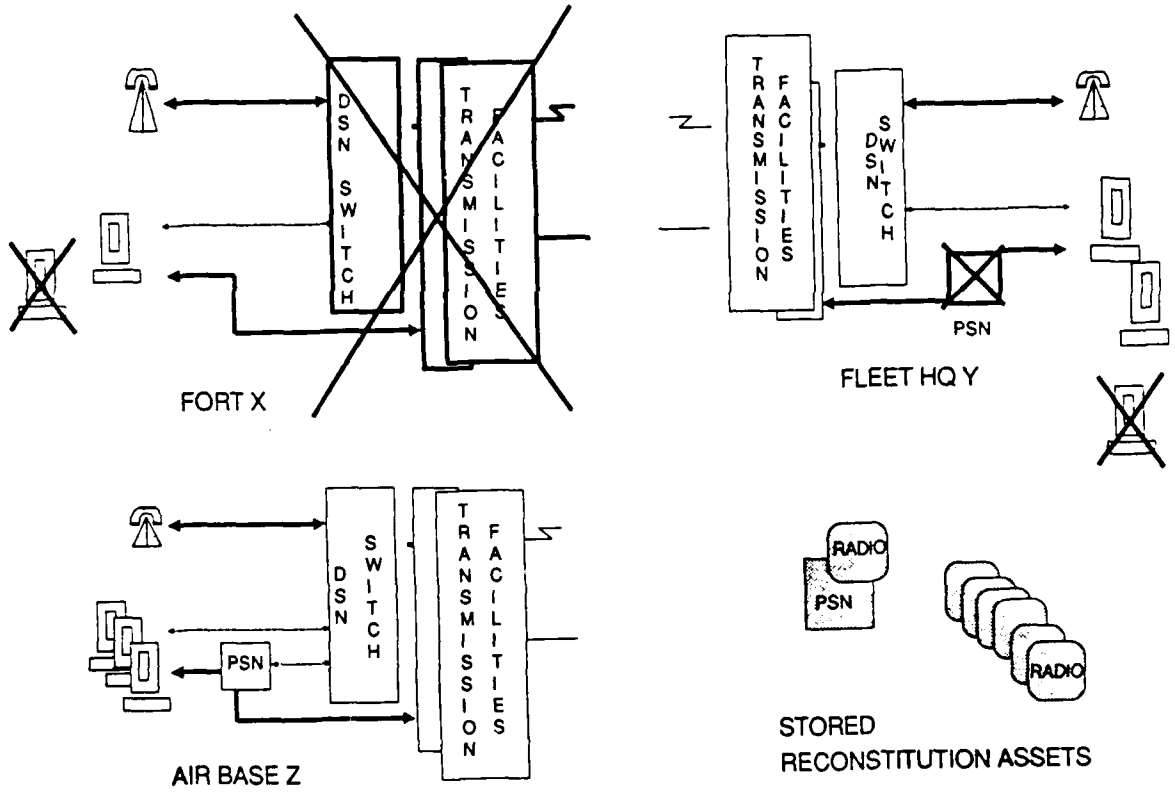


Figure 5-2. Stressed Environment

5.2.3 Reconstituted Environment

Figure 5-3 shows a potential employment configuration for use of reconstitution assets taken from a stored location within the theater. These assets have been deployed from their pre-conflict storage locations based on established procedures. This starts the process of recreating a network capable of supporting the surviving command and control elements. Personnel associated with these C^2 elements are capable of being trained to execute these reconstitution plans. The equipment must be stored with complete simplified operating instructions. Note that some subscribers may survive, but because of the pre-crisis priority system they may initially be restricted from network access. This figure shows the employment of line-of-sight radio interconnect technology primarily for subscriber access. Many variations exist to the scenario shown. The key to any reconstitution scheme lies in its adaptability to whatever the situation may be.

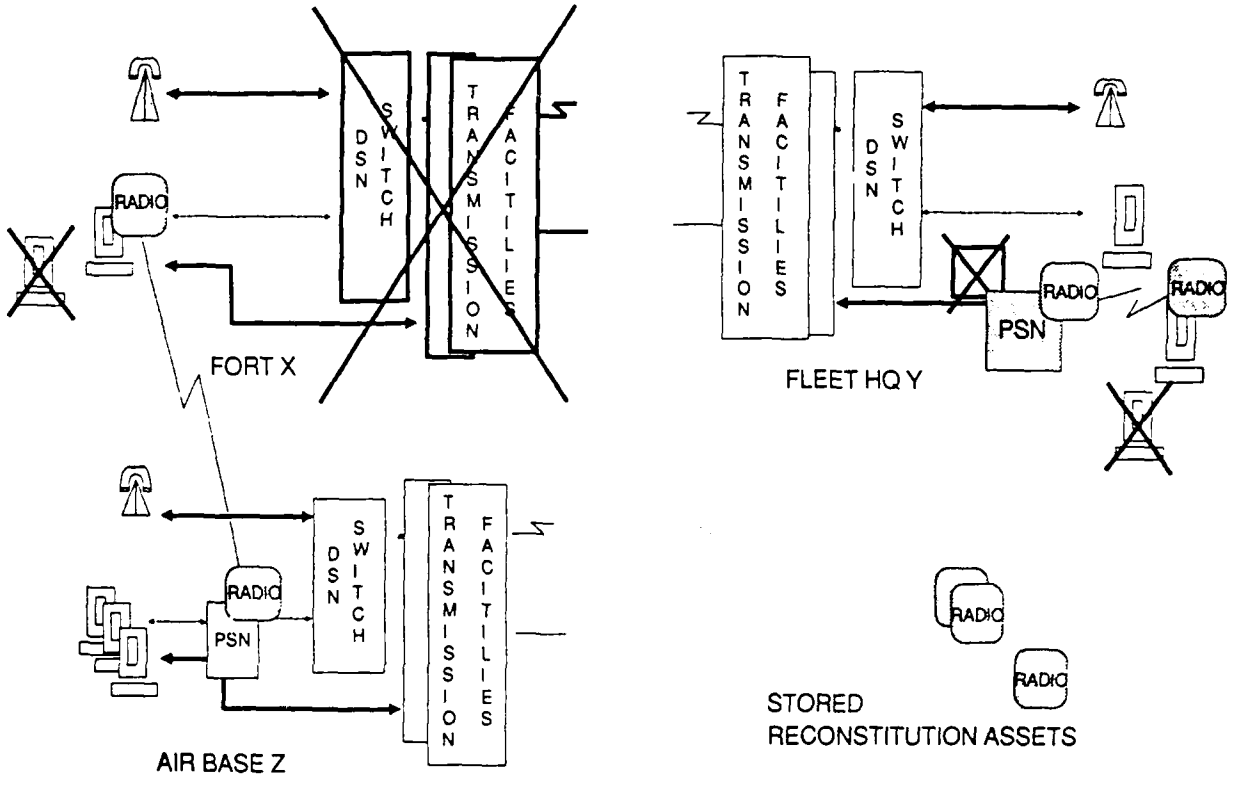


Figure 5-3. Reconstituted Environment

5.3 Potential Employment Planning Strategies

There are three potentially viable strategies that could be employed for reconstitution of data network services. They are:

1. REPAIR - Send whatever parts and people needed to repair the damaged portion of the network,

2. REPLACE - Send a self-contained switch node fully equipped with everything needed,including its own shelter, COMSEC, communications interface devices, and power system so the node can operate without external support,

3. REHOME - Rehome subscribers to an undamaged surviving switch node that is away from immediate danger. When a switch is functional but the transmission lines remain intact, the trunk circuits (ISTs) can be used to rehome priority local subscribers to a distant switch node.

The repair strategy is very manpower intensive and may find little application. It assumes that 1) the transmission facilities survived, 2) the switch equipment is repairable and can be fixed sooner than a replacement can be transported to the site and cutover to operation, and 3) the site is secure from further hostilities. The repair strategy will require a well trained cadre of technicians on standby, equipped with the parts, tools, and test equipment needed to fix each type hardware. How many crews will be necessary and how large are they? How will the people maintain their proficiency and still be available on a moments notice? Where should the teams be positioned to optimize the reaction time for each site? Who is going to assess the damage and determine the restoral equipment requirements? Is anyone available during stressed periods that is qualified and can take the time to accurately determine what node equipment is damaged, and whether it can be repaired and how long it should take? Assuming someone could make a correct assessment of the damage, there would seem to be an infinite number of possible damage scenarios. Therefore, there needs to be available in reconstitution assets, a set of spare equipment and/or parts to replace or repair each node component. How many sets/nodes? These are only some of the many questions that must be examined to properly evaluate this strategy.

The replace strategy is probably the easiest strategy to implement and manage. There is only one piece of equipment and its implementation will not change the network configuration. If we assume that the majority of service currently provided by a switching node must be reconstituted, then it make sense to either find out what the damage is and send the people and parts needed to fix it (repair strategy), or to move a complete self contained transportable node into the area and serve the surviving users. However, it does assume the availability of transmission facilities and a controlled environment. It would not be prudent to move a complete switch node deep into a hostile tactical environment that is

susceptible to more attacks. Continuing to locate reconstitution assets of any kind in a tactically insecure area could quickly reduce standby assets to zero. It is better to retain the transportable backbone switch node into a rear area and use subscriber access lines to reach the more tactically hostile enclaves of users. User traffic demands will increase during stressed periods and it will be of little value to the user to have a switch if connections through the network are blocked. Transportable nodes might also be used to temporarily augment or expand the capacity of existing nodes.

The rehome strategy requires the fewest switch nodal resources and, since it may be accomplished by the supporting carrier facility without moving in additional personnel or equipment, it can be implemented the quickest. Rehoming can restore critical service and serve as an interim fix while waiting on either the repair or replace strategies to be implemented. This strategy also assumes the availability of some supporting carrier terminal facilities and is obviously limited to the total available capacity and connectivity. When all circuits/links are not available, as is assumed in the repair and replace strategies, all subscribers can not be restored to service. This strategy requires that plans be developed that fit the established NSEP TSPS restoration procedures, Through these procedures, it should be possible to restore the critical users. It may require the pre-positioning of spare interface equipment (i.e., modems and cryptos) at the user locations for interfacing to the users equipment.

The three strategies discussed above assume the availability of some degree of supporting transmission facilities. Due to the physical links some hilltop transmission relay facilities are generally more obtrusive and accessible than switch nodes, except of course where they may be collocated within a U.S. controlled area.

To assume that all transmission facilities for either the local or the long-haul distribution will survive or be reconstituted for all users is not realistic. When data services are interrupted there is a probability that the problem may be with the interconnecting transmission plant and not the switch node. If the switching node has been damaged or destroyed there is good reason to believe that local connectivity to the network may also be damaged or destroyed.

One of the more vulnerable portions of the data network is the transmission facilities/nodes that interconnect the switching nodes. They are more numerous, accessible and, because of all the circuits (voice, data, and C^2) transiting a transmission node, a higher value target. Switch nodes are generally located within the controlled operations areas of post, camps, or stations where the user enclaves have a security force to control access. In addition, Command Center facilities are further protected by additional layers of physical security. On the other hand existing transmission nodes that serving the area are more visible (tall antennas, large sat. dishes), with relays located on remote sites that are unattended or are small and could be easily overrun or destroyed. Transmission facilities are, therefore, could be the weakest link in the survivability chain and will probability not be fully available under higher level stress scenarios.

This raises the question then of whether it is advisable to reconstitute both the switch and the transmission facilities. Existing transmission reconstitution plans will provide some connectivity needed to rehome the critical switch users to surviving nodes. These nodes would be in a safe zone and could be augmented with standby equipment without the fear of losing switch resources.

The point here is that under any attack scenario there is a very low probability that only the switch will receive damage. Therefore, reconstitution packages must consider restoral of the transmission system connectivity as well as the switching/message processing service that had existed. Restoral of the transmission facilities is a responsibility of that community and plans exist to provide connectivity service at selected users locations.

The best overall employment strategy is probably a combination of all three. However, the selection of a mix or even a single strategy mentioned above must be based on specific information relative to user needs, knowing how the user intends to operate during stressed periods, and cost trade-off analyses. It is important to know if the user will continue to operate from the same location or does he have plans to relocate if hostilities escalate, will his mission change (i.e., will there be a different community of interest), will his security requirements change, and how soon after the node is destroyed does the user need service? Does the user survive? If the user relocates, does the location remain in use by a new user community backfilled by mobilization forces?

This kind of information is essential to the planning for reconstitution and should be found in each users' Continuity of Operations Plans (COOPs). Every user that is to be reconstituted should provide a copy of his COOP to the Network Manager. This information is essential to validate the reconstitution employment strategies or strategy chosen.

5.4 Transition and Exercise Planning

Exactly how the items of equipment get deployed, who are the designated operating personnel, storage and training, and all of the detailed planning required to execute and employ any reconstitution plans/concepts are subject to a wide range of variables. As stated earlier, many other C^2 elements are also planning the development and employment of transportable communications assets for use in the stressed environment. These include subscriber terminal equipment (WWMCCS Terminals, Command Centers, etc.) and communications systems (GWEN, VLF/ELF, Airborne Platforms, etc.). To keep this document unclassified, further discussion of these programs is not possible. Any detailed planning for DCS data network reconstitution must be in total agreement and build on these national and international contingency plans. Consideration should be given to including the introduction of the future IDS data network reconstitution assets and plans in annual JCS exercises both on a worldwide and local area basis. This would permit training

on both the equipment operations and in the procedural aspects of moving the assets into place and operating them in the expected stressed environment.

This Page Left Blank Intentionally.

SECTION 6 - Summary and Recommendations

The future data network component of the DCS has three primary identifiable elements: terminals/data switches, interconnects, and operating plans/procedures. The creation of a planning strategy that addresses the question of a supporting architecture for reconstitution/restoration of data services must also be related to these three elements. The terminal/data switches and reconstitution plans and procedures are for the most part considered internal to the DCA/MILDEP data network users' community of interest, whereas the interconnect element is a component shared with the entire DCS community.

The intent of the analysis presented herein was to provide the data network engineering and planning community with an understanding and appreciation of the magnitude of the planning requirements which surround the reconstitution planning process. The provision of data services within the DoD community during all levels of stress cannot be accomplished in a vacuum. Reconstitution planning for this major data subnetwork, and principal component of the DCS, must fit within the framework of the environment in which it exists. As an operating, dependent entity of the DCS, data network reconstitution planning efforts must build on the existing plans and procedures of the DCS/NCS. One of the basic principles of systems engineering is to understand the design objectives of the whole system, while breaking problem areas down to the smallest parts and then analytically creating plans that address solutions from the ground up. This approach can be used during the creation and development of a viable strategy which addresses the reconstitution planning efforts for the current and future elements of the DCS data network.

A balanced emphasis must be placed upon all three identifiable components of the data network. While the importance of this balance is critical to the development of a complete reconstitution strategy and plan, the primary focus presented is on one of the most fundamental aspects: the physical layer of the GOSIP protocol, the interconnect media. This physical layer is the very foundation for the creation of the *System*. The development of any architecture must begin with a thorough understanding of the environment and at the roots of its intended objective. Summary comments concerning each of these three components are covered below, followed by a brief presentation of a planning framework with recommendations for the orderly incremental development of a composite reconstitution scheme.

6.1 Interconnect Media

As the shared component, interfacing the future IDS data network reconstitution interconnect requirements within the DCS planning community requires that pre-crisis restoration priorities be established commensurate with the stated mission of the end-user. Based on a set of end-user priorities, a derived priority will need to be established for the inter-switch 56 kbps trunks. The identification of the restoration priority levels begins with an in-depth analysis of the end-user mission requirements to determine traffic priorities and potential demand for service, given the end-user mission. Once this is accomplished, critical switch locations can be identified and assigned comparable restoration priorities. After this is done, an interconnect media analysis must be conducted for each identified high priority switch node location and critical cluster of high level end-user/host terminal facilities.

It is envisioned that DCS data network reconstitution planning will desire to take advantage of all appropriate media available. The selection of which interconnect media to use will depend on the specific circumstances of a wide variety of potential scenarios. Terminal/ switch nodes must be flexible and capable of interfacing with a wide variety of media. Existing and planned key nodal points should be equipped with a requisite suite of interface hardware to allow a given terminal/data switch to be interoperable with a variety of the types of interconnect media available at that specific geographical location. A basic set of information containing all the interconnect media within a 2/3 mile radius of each critical switch location must be prepared. This information should include all available information on type of media, interface requirements who owns it, and how to access the media during times of stress. These are some of the operational considerations that need to be documented. As mentioned earlier, it is possible to use a mixed blend of media in multiple link applications. The expected inventory of available interconnect media has been summarized in Section 4; there is no absolute way of determining which type of media will be available for any interested community of users. Table 4-1 contains the major categories of interconnect technologies that exist within the inventory and some of the technical parameters that must be considered if any plans are made to employ these alternatives. After identification of critical users and switches and coupled with the information on available interconnect media, it is possible that some locations will have robust connectivity while others may require augmentation through the selective acquisition of limited dedicated data network reconstitution interconnect assets, possibly similar to the LOS radio packages used in the example contained in Section 5. Under times of stress, this will not be an either/or situation; therefore, it is imperative that reconstitution planners create the most flexible and adaptable interconnect environment possible for the future Data Network.

In order for the DCS data network system to take maximum advantage of the various interconnect media, particular attention must be made to two important areas: the acquisition of the physical interface between the terminal/switch components and the

available media and the rules for establishment of appropriate restoration priority levels for an identified set of user categories.

In addition to these considerations, a lower set of throughput data rates can be expected during the initial stages of reconstitution. The data rates identified in Paragraph 2.4 are considered pre-stress day-to-day operational distances and data rates. While these can be used as reconstitution guidelines or objectives, they may not be realistically achievable in a stressed environment where the data network may be forced to use a less than optimum variety of different interconnect media.

6.2 Switch/End-User Terminal Planning

From a hardware perspective, the second component of the data network which must be addressed is the area of switch/end-user terminal facilities. After critical switch nodes are identified and prioritized, a review of the potential development and employment application of a replacement switch capability must be examined. If a requirement is identified for the development of a replacement switch capability, several key questions must be addressed concerning its potential design. Again, the systems architecture must be reviewed. Will this type of switch be employed in a tactical or strategic environment? Should this switch be developed as a transportable or mobile switch? At this time there is no known requirement for employment of a full scale packet switch in a true tactical scenario or for mobile operations. Most likely, a full scale packet switch would be employed no lower than Echelons Above Corps, a defined rear area of the theater area battlefield, and at major support headquarters locations. Individual end-user subscriber circuits may extend into the rear areas of the tactical zone to reach gateways or hosts. Given this application, a need is envisioned for the development of a transportable packet switch node which is capable of use as either a replacement or augmentation asset. Any transportable packet switch node that might be developed for this use in the future IDS switched network environment must be assembled as a total *package* and not just a switch in a truck. This package should include (1) the packet switch, (2) a complete suite of ancillary equipment equal to the most complex pre-crisis operational switch node (a DISNET packet switch node), (3) multi-level and link encryption devices, (4) interface and end-to-end protocol suite, as required, and (5) communications interface hardware for interconnecting with any potentially surviving backbone elements as derived from the interconnect analysis addressed in the previous section. Additionally, the transportable packet switch node will require pre-positioned, well documented procedural instructions, and an information base that has been designed for the specified area of operation. The logic behind selection of the most complex pre-crisis switch hardware configuration lies in the capabilities. A transportable DISNET-equipped switch can function as either a DISNET or MILNET replacement; however, a MILNET data switch can only be used on the MILNET subsystem.

6.3 Plans and Procedures

The purpose of planning is *not* to tell you what you - or your successor - should do five or ten years from now. It is to tell you what you have to do *today* in order to have a desired capability five or ten or fifteen years from now. The plans and procedures which address the total spectrum of reconstitution planning are considered to be multi-layered and multi-faceted. The plans that document the hardware considerations mentioned in the above two subsections are, but a fraction of the required documentation necessary to address the re-constitution question.

In addition to the reconstitution plans that surround the question of "What" should be done to prepare for reconstitution, another dimension of planning effort must also be addressed, that of "How" to operate the data network during times of stress. This planning dimension can be categorized as the instructions and guidance necessary to operate in the expected environment. In a network that has few if any operating personnel, (most of the switches will be unmanned) the procedures for reconnecting the surviving customers to a surviving switch and into the available interconnecting media will not be an easy task. One of the largest questions here is "Who" is going to orchestrate the network/local area restoration activities and "Who" is going to accomplish the actions required to recreate the data services network. Many of the surrounding communications facilities are converting to streamlined digital, less manpower intensive equipment. Those operating communications personnel that do remain on site will be fully employed reconstituting and maintaining critical high level command and control traffic. The requirements of the general services data network must be placed in perspective with all other telecommunications services and handled accordingly. The process of reestablishing the requisite data bases and identifying addresses and subscribers must be made as simple as possible. Potentially encryption devices may have to be by-passed during the initial stages of reestablishing the net. Simple equipment recognition signaling should be used with pre-determined operator identification codes. These methods will allow for hand shake recognition of both the equipment and the operators to begin the process of interconnecting whatever surviving assets that remain operational. After some reasonable level of network has been reestablished, return to the day-to-day operating procedures should be accomplished as soon as possible.

The basic reconstitution matrix, introduced as Figure 2-6, can be used as a preliminary guide, but care must be taken that the plans for each of the identifiable components of the data network are integrated and address a composite data network architecture that will function adequately during times of stress. The reconstitution matrix can be used as an architectural framework around which portions of the total reconstitution plan can be developed.

6.4 Recommendations

As a result of the analysis of relationships and data network components, it is recommended that reconstitution engineering/planning emphasize and focus on the following areas:

1. Coordinate with the proper activities (FEMA/NCA) to resolve any differences in identified stress levels to be used in developing the interconnect priorities

2. Pre-war establishment of a plan for restricting user access into the network by means of a priority precedence system

3. Pre-crisis assignment of circuit restoral priorities for subscriber, access area, and inter-packet switch trunks in accordance with established reconstitution plans of the DCS and the National Command Authorities (NCA) for the specified area of operation

4. The identification and incremental acquisition of an appropriate suite of communications devices (including interconnect/interface devices, radios), software (for control and protocols), and modems/cables necessary to interface a packet switch node with any surviving transmission or voice switch facilities

5. The design and potential development of a transportable packet switch node capability for use as a replacement or restoral of damaged or impaired pre-war packet switch nodes, as discussed above

6. The development of a local area interconnect capability, potentially a small portable low frequency line-of-sight radio, to provide dedicated local area connectivity on a end-user/host-to-switch basis

7. The identification of a recommended suite of host/terminal equipment for subscriber interconnect during the post-war time frame. Simple straight forward terminal facilities will be more appropriate than the more complex end-users.

8. Documentation of the post-crisis system operational plans/procedures and security considerations including subscriber/host identification and reconnect procedures for reconstitution of the operating data subnetwork of the DCS. This includes development of new address databases and how to implement, etc.

These items, when addressed and taken in their composite form will go a long way toward answering the spectrum of reconstitution planning for the data services network component of the DCS. The development of any precise data network reconstitution plan requires a

through understanding of and access to established multi-level MILDEP, CINC, DoD, National (FEMA), and International contingency plans. Most of these plans are extremely sensitive and highly classified and were not available as input for this analysis. Therefore, other than the identification of the above listed items, no additional "road map" or strategy can be documented at this time. The DCS Data Systems Office in conjunction with its supporting engineering activity (DCEC) must determine the appropriate planning responsibilities associated with the creation of actual reconstitution plans.

This Page Left Blank Intentionally.

Appendix A

Glossary of Terms

1. AFM 11-1, Vol I, 2 January 1976:

Command and Control Communications: All telecommunications systems employed to satisfy functions of command, control, and day-to-day operation of mission forces.

Common-User Communications: Voice and record communications systems, networks and facilities established and operated to serve the general needs of Department of Defense agencies for electrical exchange of common categories of information, e.g., administrative, logistical, personnel, etc. (some examples of common-user communications are AUTODIN, AUTOVON, and AUTOSEVOCOM).

2. AFM 11-1, Vol III, 15 November 1973:

Mobile: As applied to an equipment, facility, or major element of a system, capable of performing the intended mission while in motion.

System: Generally, a term used to describe communication facilities form an engineering point of view and includes all associated equipment. More specifically, two or more physically separated but interrelated and interdependent C-E facilities that perform a clearly defined function to fulfill an established requirement. It includes all related facilities, equipment, material, services, and personnel essential to its operation and maintenance.

Tactical communications systems: Systems which provide internal communications within tactical elements, composed of transportable and mobile equipment assigned as unit equipment to the supporting tactical unit.

Transportable: As applied to an equipment, facility, or major element of a system, designed to be readily transported from one location to another but not capable of performing the intended mission while being so transported.

3. Army Technical Manual 11-486-1, 7 August 1963:

Mobile Transmitter: A radio transmitter designed for installation in a vessel, vehicle, or aircraft, and normally operated while in motion.

Transportable Transmitter: Radio transmitting and receiving system, a transportable transmitter is a transmitter designed to be readily carried or transported from place to place, but which is not normally operated while in motion.

4. Army Regulation 310-25, 21 May 1986

Strategic Communications: Continental, intercontinental, and intercommand telecommunications facilities and services that are owned, leased, operated, or controlled by the Department of the Army, which provide a means for the exercise of command and control, and logistic and administrative support of elements of the Department normally assigned down to the Army component commander within the theater of operations, (Echelons above Corps) and other Department of Defense and Governmental agencies as directed.

Tactical: Pertaining to the employment of units in combat.

Tactical communications: Communications provided by, or under the operational control of, commanders of combat forces, combat troops, combat support troops, or forces assigned a combat service support mission.

5. Telephony Dictionary of Communications Terms, James Holmes, Editor, 1986:

Mobile: Transmitter designed for installation in a vessel, vehicle, or aircraft and normally operated while in motion.

Transportable: Transmitter designed to be readily carried or transported from place to place, but which is not normally operated while in motion.

6. Glossary of Telecommunications Terms-Federal Standard 1037, July 1980:

Communications System: A collection of individual communications networks, transmission systems, relay stations, tributary stations, and terminal equipment capable of interconnection and interoperation to from an integral whole, i.e., the Defense Communications System (DCS). NOTE: These individual components must serve a common purpose, be technically compatible, employ common procedures, respond to some form of control, and in general, operate in unison.

Tactical Communications: A method or means of conveying information of any kind, especially orders and decisions from one command, person, or place to another within the tactical forces, normally by means of electronic equipment (including communications security equipment) organic to the tactical forces. NOTE: Excluded from this definition are communications provided to tactical forces by DCS, to nontactical forces by DCS, to tactical forces by nontactical military commands, and to tactical forces by civil organizations.

7. DCAC 310-70-1, DCS Systems Control, Volume I, Policy and Responsibilities, August 1986.

DCS Facility: A DCS facility is any facility that has been identified as a DCS facility in DCAC 310-70-61 "Identification of Components of the DCS." It could be a Government-owned or a combination of Government-owned, fixed, transportable, mobile assets or leased equipment, as appropriate, that provide general purpose, long-haul, point-to-point transmission media system, traffic switching function, or communications support capability.

DCS Station: A DCS station composed of one or more DCS facilities operated and maintained by the Government or a contractor through which or to which DCS or a combination of DCS/non-DCS communications links, trunks, or circuits pass or terminate. A DCS station can accomplish a variety of functions including terrestrial or satellite transmission, message switching, circuit switching, circuit restoration, rerouting, trouble isolation, repair, circuit coordination, or facility coordination. (DSN Switch and DDN PSN fall into this category.)

Technical Control Facility (TCF): The TCF is the part of a DCS station that functions as the interface between the transmission elements of the DCS and the users of the system. It has the physical and electrical capabilities necessary to perform the required functions of technical control.

This Page Left Blank Intentionally.

Appendix B

List of Acronyms

A/D	Analog to Digital
ANSI	American National Standards Institute
AO&M	Administration, Operation, and Maintenance
AO&M/NM	Administration, Operation, and Maintenance/Network Management
ARPANET	Advanced Research Project Agency Network
AT&T	American Telephone and Telegraph Company
ATE	Automated Test Equipment
AUTODIN	Automatic Digital Network
AUTOVON	Automatic Voice Network
C^2	Command and Control
C^3	Command, Control, Communications
CCITT	Consultative Committee International Telephone and Telegraph
DACS	Digital Crossconnect System
dB/K	Decibel per Kelvin
dBW	Decibels referenced to one Watt
DCA	Defense Communications Agency
DCAC	Defense Communications Agency Circular
DCEC	Defense Communications Engineering Center
DCOSS	Defense Communications Operational Support System
DCS	Defense Communications System
DCTN	Defense Commercial Telecommunications Network
DDN	Defense Data Network
DDS	Digital Data System
DECCO	Defense Commercial Communications Office
DISNET	Defense Integrated Secure Network
DOCS	DSCS Operations Control System
DoD	Department of Defense
DPAS	Digital Patch and Access System

DSCS	Defense Satellite Communications System
DSN	Defense Switched Network
DSNET1	Defense Secure Network 1
DSNET2	Defense Secure Network 2
DSNET3	Defense Secure Network 3
DTN	Digital Transmission Network
E^3	End-to-end encryption
EIRP	Effective Isotropic Radiated Power
GHz	Gigahertz
HF	High Frequency
ICF	Interconnect Facility
IDSCP	DCS Integrated System Control Program
IEEE	Institute of Electrical and Electronic Engineers
ISDN	Integrated Services Digital Network
ISO	International Organization for Standards
ISO-OSI	International Organization for Standards - Open System Interconnect
JTC^3A	Joint Tactical Command, Control, and Communications
kbps	Kilobits per second
LOS	Line of Sight
Mbps	Megabits per second
MC	Monitoring Center
MHz	Megahertz
MIL-HDBK	Military Handbook
MIL-STD	Military Standard
MILDEP	Military Department
MILNET	Military Network
MOU	Memorandum of Understanding
NBS	National Bureau of Standards
NCS	National Communication System
NCSC	National Computer Security Center
NETS	National Emergency Telecommunications System
NSA	National Security Agency
O&M	Operations and Maintenance
OSI	Open System Interconnect (see ISO-OSI)
PCM	Pulse Code Modulation

STU	Secure Telephone Unit
SVP	Secure Voice Program
SVS	Secure Voice System
T1	North American DS1 rate of 1.544 Mbps $\pm$ 75 bps signal standard
TAC	Terminal Access Controllers
TCF	Technical Control Facility
TCSEC A1	Trusted Computer System Evaluation Criteria Class A1
TCSEC B1	Trusted Computer System Evaluation Criteria Class B1
TCSEC B2	Trusted Computer System Evaluation Criteria Class B2
TCSEC B3	Trusted Computer System Evaluation Criteria Class B3
TCSEC C2	Trusted Computer System Evaluation Criteria Class C2
TEMP	Test Evaluation Master Plan
TRAMCON	Transmission Monitor and Control
TROPO	Tropospheric Scatter
VF	Voice Frequency
VSAT	Very Small Aperture Terminal
WWDSA	World Wide Digital System Architecture
WWMCCS	World Wide Military Command & Control System
WWOLS	World Wide On-Line System

This Page Left Blank Intentionally.

Appendix C

Levels of Stress

The tables included in this appendix present two different definitions of levels of stress. Table C-1 below compares the stress levels and equates one to the other; Table C-2 presents the DDN Program Plan (1982) stress levels; and Table C-3 presents the National Security Emergency Preparedness Telecommunications Service Priority System (NSEP TSPS) stress level descriptions.

Table C-1. DDN/NSEP TSPS Stress Level Comparison

DDN \ TSP	Peacetime/ Crisis/ Mobilization	Attack/ War	Post-Attack/ Recovery
Peacetime/Readinesss	X		
Crisis and Pre-attack and Theater Non-Nuclear War	X	X	
Early Trans. Attack (few weapons, possibly HEMP)		X	
Massive Nuclear Attack		X	
Post Attack			X

Table C-2. DDN Program Plan Stress Level Descriptions

STRESS LEVEL	RANK	PRIMARY DDN ROLE	MAJOR THREATS	SURVIVABILITY FEATURES
A. Peacetime, Readiness	4	Support Command and Control and Intelligence traffic and DoD Administrative users	1. Random failures due to wearout of hardware components, residual software bugs, and external failures (e.g., A/C failure)	Network design - Network dispersion - Redundancy - Dynamic routing
B. Crisis and Pre-Attack, and Theater Non-Nuclear War	1	Above, plus surge requirements, handled according to established precedence	1. Surge in traffic load 2. Random failures 3. Sabotage 4. Use of conventional weapons against the network elements in Europe	- As above, and - Precedence/preemption - Reconstitution nodes - Preplanned alternative circuit routing - Preplanned rehoming
C. Early Trans-Attack (Few Weapons Possibly HEMP)	2	Support Critical C2I Traffic	1. HEMP 2. Use of few nuclear weapons against the system assets in CONUS	- As above, and - HEMP hardening - Site hardening when collocated with hardened users - User COOP plans
D. Massive Nuclear Attack	5	Support Critical C2I Traffic as able	1. Extensive use of nuclear weapons against the system assets in CONUS	- As above
E. Post-Attack	3	Possess capability to initiate reconstitution from the surviving fragments of the DDN. Support the DCS as part of the NCS in reconstituting national communications	1. Possible use of few nuclear weapons against the surviving system elements	- As above, and - Rehoming existing IS/A AMPES and interconnecting them - Reconstitution MC

Table C-3. National Security Emergency Preparedness Telecommunications Service Priority System Stress Level Descriptions

CATEGORY	PEACETIME/ CRISIS/ MOBILIZATION	ATTACK/ WAR	POST-ATTACK/ RECOVERY
EMERGENCY NSEP	PP[1]	PP	PP
a. Presidentially-declared (Disaster Relief Act) b. State or locally declared c. NCA-declared crisis (e.g., War) d. Protection of endangered U.S. personnel or property e. Damaged NSEP facilities f. Critical to National Security as certified by Agency head, etc. g. Court orders issued per FISA			
ESSENTIAL NSEP	PP RP[2]	PP RP	PP RP
National Security Leadership a. Critical orderwire or control service b. Presidential communications for continuity of government and national leadership during crisis situations c. NCA communications for military command and control critical to national survival d. Intelligence communications for catastrophic attack warning e. Communications for Diplomatic negotiations for arresting or limiting hostilities			
NATIONAL SECURITY POSTURE AND U.S. POPULATION ATTACK WARNING a. Threat assessment and attack warning b. Conduct of diplomacy c. Intelligence collection, processing, and dissemination d. Command and control e. Continuity of state and local government functions supporting the Federal government during and after national emergencies			

Priority Level Assignments

Emergency NSEP. Telecommunication services in the Emergency NSEP category are those new services so critical as to be required to be provisioned at the earliest possible time, without regard to the cost of obtaining them.

(1) Services qualifying under the Emergency NSEP category are assigned priority level "E" for provisioning.

(2) After 30 days, assignments of provisioning priority level "E" for Emergency NSEP services are automatically revoked unless extended for another 30-day period.

(3) For restoration, Emergency NSEP services may be assigned priority levels under the provisions applicable to Essential NSEP services. Emergency NSEP services not otherwise qualifying for restoration priority level assignment as Essential NSEP may be assigned a restoration priority level "5" for a 30-day period.

Priority Level Assignment

National Security Leadership. This subcategory will be strictly limited to only those telecommunication services essential to national survival if nuclear attack threatens or occurs, and critical orderwire and control services necessary to ensure the rapid and efficient provisioning or restoration of other NSEP telecommunication services. Services in this subcategory are those for which a service interruption of even a few minutes would have serious adverse impact upon the supported NSEP function. Services under this subcategory will normally be assigned, during Peacetime/Crisis/Mobilization, priority level "1" for provisioning and restoration.

Priority Level Assignment

National Security Posture and U.S. Population Attack Warning. This subcategory covers those minimum additional telecommunication services essential to maintaining an optimum defense, diplomatic, or continuity-of-government posture before, during, and after crisis situations. Services in this subcategory are those for which a service interruption ranging from a few minutes to one day would have serious adverse impact upon the supported NSEP function. Services under this subcategory will normally be assigned, during Peacetime/Crisis/Mobilization, priority levels "2," "3," "4," or "5" for provisioning and restoration.

and attack warning
b. Conduct of diplomacy
c. Intelligence collection, processing, and dissemination
d. Command and control
e. Continuity of state and local government functions supporting the Federal government during and after national emergencies
f. National space operations

PUBLIC HEALTH, SAFETY, AND MAINTENANCE OF LAW AND ORDER

a. Population warning (other than attack warning)
b. Law enforcement
c. Continuity of critical state and local government functions (other than those supporting the Federal government during and after national emergencies
d. Hospitals and distribution of medical supplies
e. Critical logistic functions and public utility service
f. Civilian Air Traffic Control
g. Military assistance to civil authorities
h. Defense and protection of critical industrial facilities
i. Critical weather services
j. Transportation to accomplish the foregoing

PUBLIC WELFARE AND MAINTENANCE OF NATIONAL ECONOMIC POSTURE

a. Distribution of food and other essential supplies
b. Maintenance of national monetary, credit and financial systems
c. Maintenance of price, wage, rent, and salary stabilization, and consumer rationing programs
d. Control of the production and distribution of strategic materials and energy supplies
e. Prevention and control of environmental hazards or damage
f. Transportation to accomplish the foregoing

National Security Posture and U.S. Population Attack Warning. This subcategory covers those minimum additional telecommunication services essential to maintaining an optimum defense, diplomatic, or continuity-of-government posture before, during, and after crisis situations. Services in this subcategory are those for which a service interruption ranging from a few minutes to one day would have serious adverse impact upon the supported NSEP function. Services under this subcategory will normally be assigned, during Peacetime/Crisis/Mobilization, priority levels "2," "3," "4," or "5" for provisioning and restoration.

Priority Level Assignment

Public Health, Safety, and Maintenance of Law and Order. This subcategory covers the minimum number of telecommunication services necessary for giving civil alert to the U.S. population and maintaining law and order and order and the health and safety of the U.S. population in times of any national, regional, or serious local emergency. These services are those for which a service interruption ranging from a few minutes to one day would have serious adverse impact upon the supported NSEP functions. Services under this subcategory will normally be assigned, during Peacetime/Crisis/Mobilization, priority levels "3," "4," or "5" for provisioning and restoration.

Priority Level Assignment

Public Welfare and Maintenance of National Economic Posture. This subcategory covers the minimum number of telecommunication services necessary for maintaining the public welfare and national economic posture during any national or regional emergency. These services are those for which a service interruption ranging from a few minutes to one day would have serious adverse impact upon the supported NSEP function. Services under this subcategory will normally be assigned, during Peacetime/Crisis/Mobilization, priority levels "4" or "5" for provisioning and restoration.

NOTES:

1 PP - Provisioning Priority

2 RP - Restoration Priority

Table C-3. National Security Emergency Preparedness Telecommunications Service Priority System Stress Level Descriptions

CATEGORY	PEACETIME/ CRISIS/ MOBILIZATION	ATTACK/ WAR	POST-ATTACK/ RECOVERY
EMERGENCY NSEP	PP[1]	PP	PP
a. Presidentially-declared (Disaster Relief Act) b. State or locally declared c. NCA-declared crisis (e.g., War) d. Protection of endangered U.S. personnel or property e. Damaged NSEP facilities f. Critical to National Security as certified by Agency head, etc. g. Court orders issued per FISA			
ESSENTIAL NSEP	PP RP[2]	PP RP	PP RP
National Security Leadership			
a. Critical orderwire or			

Priority Level Assignments

Emergency NSEP. Telecommunication services in the Emergency NSEP category are those new services so critical as to be required to be provisioned at the earliest possible time, without regard to the cost of obtaining them.

(1) Services qualifying under the Emergency NSEP category are assigned priority level "E" for provisioning.

(2) After 30 days, assignments of provisioning priority level "E" for Emergency NSEP services are automatically revoked unless extended for another 30-day period.

(3) For restoration, Emergency NSEP services may be assigned priority levels under the provisions applicable to Essential NSEP services. Emergency NSEP services not otherwise qualifying for restoration priority level assignment as Essential NSEP may be assigned a restoration priority level "5" for a 30-day period.

Priority Level Assignment

National Security Leadership

END

DATE

FILMED

9-88

DTIC